# Intelligence cyber : intégrer les hackers dans une stratégie de sécurité numérique globale. Le modèle de l'intelligence économique

Yannick Pech

# Université de Poitiers

École Doctorale 526 SORG - ED8 SSTSEG
UR 13564 – Laboratoire CEREGE

* * *

Thèse de doctorat
en Sciences de l'information et de la communication

---

***Intelligence cyber :***
***intégrer les hackers dans une stratégie de sécurité numérique globale.***
***Le modèle de l'intelligence économique.***

---

**Yannick Pech**

Soutenue le 20 décembre 2023, sous la direction du Professeur Nicolas Moinet.

***Membres du jury*** :

**Christophe Assens**, *Professeur à l'Université de Versailles Saint-Quentin-en-Yvelines* (rapporteur)
**Christian Bourret**, *Professeur à l'Université Gustave Eiffel* (rapporteur)
**Ludovic François**, *Professeur affilié à HEC Paris*
**Stéphane Goria**, *Maître de Conférences HDR à l'Université de Lorraine*
**Nicolas Moinet**, *Professeur à l'Université de Poitiers* (directeur de thèse)

« *Il y a une relation d'amour-haine entre l'État et les hackers. Parce que ceux qui les diabolisent sont les mêmes qui les utilisent largement. Les hackers sont les seuls capables de contrebalancer et de jouer dans la même cour que les États invasifs et les entreprises dévoreuses de données. On voit les hackers comme des héros, alors pourquoi dans le même temps continuer à les considérer comme les méchants ?* […] *Les hackers sont ceux qui peuvent aider à reprendre le contrôle sur les technologies et les adapter. On peut voir la matrice, et cela donne un avantage pour comprendre comment elle marche vraiment. On a besoin de subvertir les technologies pour les renforcer et les améliorer.* »

Keren Elazari

# REMERCIEMENTS

Il est coutume de dire que le parcours du « thésard » est loin de s'apparenter à un long fleuve tranquille, voire qu'il relève du parcours du combattant. Le sentier que nous avons frayé ne fait pas exception, entre aléas de la vie, hésitations, motivation et ténacité. Le travail ici présenté n'aura pas bénéficié de tout le soin que nous aurions voulu y apporter. Toutefois, nous l'avons mené au mieux et en sommes pour cela reconnaissant auprès de nombreuses personnes.

En premier lieu, j'aimerais remercier chaleureusement le Professeur Nicolas Moinet de m'avoir dirigé et ainsi permis de faire aboutir un projet personnel envisagé de longue date. L'image qui me vient immédiatement à l'esprit à son endroit est celle d'un mentor doté précisément de *l'esprit commando*. Optimisme pragmatique, humour, modestie, intelligence fine, leadership discret me semblent caractériser au mieux ce praticien-chercheur inspirant. Merci encore pour ta confiance et ton amitié.

Ensuite, je tiens à adresser mes remerciements à Laurence Sauvêtre-Autin dont le professionnalisme, la bienveillance et la disponibilité ont été d'une aide certaine dans la gestion d'aspects administratifs liés au doctorat.

Par ailleurs, cette thèse n'aurait pas vu le jour sans le temps et les témoignages qu'ont bien voulu m'octroyer et livrer les personnes avec qui je me suis entretenu. Ils forment le corps et la substance de ce travail. Sans pouvoir tous les citer, je pense notamment à Julien Métayer et Alexandre Oda, électrons libres réactifs et ouverts ; à Florent Curtet, un esprit engagé et drôle; Yohann Bauzil, compagnon de la RCCO toujours à l'écoute ; le général Christophe Gomart pour son accessibilité (par deux fois dans ma carrière d'apprenti-chercheur) et son expérience; Guillaume Poupard, pour son amabilité, humilité et sa sincérité ; Victor Poucheret, jeune esprit éloquent en plus d'un hacker surdoué ; Pierre Penalba pour son expérience et sa vision éclairante et éclairée. Qu'ils soient ici remerciés. Ma gratitude va également à tous ceux que je ne puis citer ici, mais qui m'ont beaucoup apporté par leurs savoir et expérience, tous différents mais complémentaires.

Enfin, je remercie ma famille pour son soutien indéfectible et notamment dans les moments délicats.

# RÉSUMÉ

Placée au défi de la cybersécurité, la France semble accuser le coup. La cybermenace montre l'hybridation toujours plus néfaste d'attaques informatiques et d'offensives plus immatérielles que l'on peut assimiler à une cyberguerre et une guerre informationnelle. Or, si des initiatives publiques voient le jour depuis quelques années pour y faire face, nombre de spécialistes pointent le manque de coordination et de politique intégrée en la matière. C'est l'objet de cette thèse qui cherche à sonder les liens qui unissent les autorités étatiques et organisations privées avec un profil particulier d'expert en sécurité numérique : les hackers. En effet, ces derniers ne constituent-ils pas le chainon manquant de la stratégie de cybersécurité nationale ? Dans une première partie, ce travail fait un état des lieux de cette stratégie et propose d'appréhender la culture et l'état d'esprit propres aux hackers. Puis, après avoir étudié le concept d'intelligence économique, la deuxième partie en identifie les caractéristiques-clés pour modéliser une grille de lecture à partir de laquelle sont appréhendés les enjeux du cyber. Enfin, la troisième partie soumet à notre grille de lecture quatre cas d'étude des rapports qu'entretiennent hackers et institutions, puis propose le concept d'*Intelligence cyber* comme horizon stratégique à suivre. De là sont formulées des préconisations pour une cybersécurité nationale offensive et un État-cyberstratège.

Ce travail de recherche permet de constater que les relations qu'entretiennent hackers et organisations publiques et privées sont de nature utilitariste et, qu'en dépit de l'ouverture opérée dans leur direction, ils ne sont pas pleinement intégrés dans une stratégie de cybersécurité nationale.

**Mots-clés :** *hacking – cybersécurité – intelligence cyber – intelligence économique – stratégie – géoéconomie – géopolitique – cyberdéfense – cyberguerre – infoguerre – renseignement – OSINT.*

# ABSTRACT

Faced with the challenge of cybersecurity, France seems to be powerless. The cyberthreat shows the increasingly harmful hybridisation of computer attacks and more intangible offensives that can be likened to cyberwarfare and information warfare. Yet, although public initiatives have been launched in recent years to deal with this, many specialists point to the lack of coordination and integrated policy in this area. The aim of this thesis is to explore the links between state authorities, private organisations, and a particular type of digital security expert: hackers. Indeed, aren't hackers the missing link in our country's cybersecurity strategy? In the first part of this paper, we take stock of this strategy and look at the culture and mindset of hackers. Then, after studying the concept of economic intelligence, the second part identifies its key characteristics to model a reading grid from which to apprehend the challenges of cyber. Finally, the third part applies our reading grid to four case studies on the relationship between hackers and institutions, and then proposes the concept of *Cyber Intelligence* as a strategic horizon to be followed. This leads to recommendations for an offensive national cybersecurity and a cyberstrategist-State.

Through this research it appears that the relationship between hackers and public and private organisations is utilitarian in nature and that, despite the openness towards them, they are not fully integrated into a national cybersecurity strategy.

**Keywords :** *hacking – cybersecurity – cyber intelligence – economic intelligence – strategy – geoeconomics – geopolitics – cyberdefence – infowars – intelligence – OSINT.*

# TABLE DES SIGLES ET ACRONYMES

**ANSSI :** Agence nationale de la sécurité des systèmes d'information.
**APT :** *Advanced Persistent Threat*.
**CCC :** *Chaos Computer Club*.
**COMCYBER/COMCYBERGEND :** Commandement de la cyberdéfense/de la gendarmerie.
**CTI :** *cyber threat intelligence*.
**DGSE :** Direction générale de la sécurité extérieure.
**DGSI :** Direction générale de la sécurité intérieure.
**DRM :** Direction du renseignement militaire.
**DRSD :** Direction du renseignement de la sécurité de la Défense.
**ECIm :** Effets dans les Champs Immatériels.
**EUA :** États-Unis d'Amérique.
**FIC :** Forum international de la cybersécurité.
**GAFAM/GAMAM :** Google-Apple-Facebook-Microsoft ; Google-Apple-Meta-Microsoft.
**GCHQ :** *Government Communications HeadQuarters*.
**GEOINT :** *Geospatial Intelligence*.
**HUMINT/ROSO :** *Human Intelligence*/renseignement d'origine source humaine
**ISP/FAI :** Internet Service Provider/fournisseur d'accès à Internet.
**L2I :** Lutte informatique d'influence.
**LID/LIO :** Lutte informatique défensive/Lutte informatique offensive.
**MINARM/MININT :** Ministère des Armées/Ministère de l'Intérieur.
**NATU :** Netflix, Airbnb, Tesla et Uber.
**NCW :** *Network Centric Warfare*.
**NSA :** *National Security Agency*.
**OSINT/ROMESO :** *Open Source Intelligence*/renseignement d'origine média sociaux
**PoC :** *Proof of Concept*.
**RI :** relations internationales.
**RMA :** *Revolution in Military Affairs*.
**RSN :** réseaux socionumériques.
**SCADA :** *Supervisory Control and Data Acquisition*.
**SGDSN :** Secrétariat général de la Défense et de la Sécurité nationale.
**SIEM :** Security Information Event Management.
**SIGINT/ROEM :** *Signal Intelligence*/renseignement d'origine électromagnétique.
**SOC :** *Security Operations Center*.
**SR :** service de renseignement.
**USCYBERCOM :** *United States Cyber Command*.
**VoIP :** *Voice over InternetProtocol*.
**VPN :** *Virtual Private Network*.

# SOMMAIRE

# INTRODUCTION

*Les hackers rêvent-ils de moutons numériques ou de cyber-stratégie ?*

On sait du moins que leurs pérégrinations oniriques sont jalonnées d'aspirations à la liberté : liberté de l'information, de la communication, de la diffusion du savoir et de la connaissance, liberté d'agir sans autorisation. Mais qui sont précisément ces profils anticonformistes dont le crédo pourrait se traduire par la formule de Richard Stallman, père du logiciel libre : « *hacker, c'est s'amuser dans l'usage de son intelligence* » ? S'agit-il de pirates informatiques ennemis de la démocratie ou faut-il les voir au contraire comme des citoyens engagés et le système immunitaire de notre monde numérique ? Les hackers sont en fait des passionnés qui voient le monde comme un terrain de jeu où l'ordinateur et la technologie doivent se placer au service de la liberté du plus grand nombre, et améliorer l'existence humaine « *pour créer la civilisation de l'esprit* »[1]. Or, pour cela, il faut maitriser l'ordinateur, en sonder le fonctionnement, en explorer les entrailles électroniques. Ces explorateurs de l'informatique cherchent ainsi constamment à contourner, pousser à leurs retranchements ces machines afin de les améliorer. Navigateurs placés à l'intersection des univers virtuel et réel, leur approche est tout à la fois scientifique, expérimentale et ludique. Pour eux, créateurs du cyberespace, ce monde nouveau numérique est une utopie, à la fois lieu immatériel et idéal.

Mais ce lieu indéfini devient progressivement une dystopie, ou plutôt le voile d'une illusion scintillante qui se lève et masquait difficilement une réalité plus amère. Le monde physique et ses imperfections se projettent naturellement en une réalité augmentée dans ce monde numérique. Cybercriminalité, cyberguerre, cyberdéfense, cybersécurité… les substantifs associés à cet espace témoignent d'une hybridation des enjeux où l'information analogique ou numérique, loin d'être libre et intègre, est attaquée de toutes parts : niée, dissimulée, détruite, altérée, subtilisée, monnayée. Les guerres de l'information[2] par les contenants et les contenus, par la technique et la technologie ont trouvé le milieu parfait pour s'épanouir, dans un contexte de guerre systémique où les rapports de force et d'influence entre

[1] John Perry Barlow, https://www.eff.org/cyberspace-independence.

[2] Voir Olivier Coussi, Audrey Knauf, Nicolas Moinet, « Les guerres pour, par et contre l'information », *Revue internationale d'intelligence économique*, 2021/1 (Vol. 13), 184 p., ou encore Céline Marangé & Maud Quessard, *Les guerres de l'information à l'ère numérique*, PUF, 2021, 456 p.

tous les acteurs se durcissent. Attaques informatiques et offensives informationnelles se combinent dans une optique d'efficacité et une logique d'impact.

Face à ces enjeux, où et comment se positionne la France ? Toutes les dix secondes, en effet, une attaque par rançongiciel a lieu sur notre territoire. Sans oublier les grands groupes, les principales cibles de ces cyber-offensives sont en 2022 les PME (90% des attaques), ETI et TPE (40% au total des trois), les collectivités territoriales (23%) et les établissements de santé (10%) pour un total de pertes estimé à plus de 2Mds€[3]. Si les *ransomwares* sont les maliciels[4] les plus utilisés par les criminels, la cybermenace se diversifie et des armes numériques viennent, au-delà de la cybercriminalité, nourrir ce qui s'apparente de plus en plus à une véritable cyberguerre[5]. L'Agence nationale de la sécurité des systèmes d'information (ANSSI*) note qu'une convergence des outils et méthodes de plus en plus forte s'opère entre les acteurs du crime numérique et ceux de la guerre informatique. Or, ces acteurs malveillants hybrides évoluent et gagnent en maturité et expertise, engendrant une pression toujours plus forte sur la société et une difficulté à caractériser leurs activités et opérations. En effet, les attaquants visent désormais des cibles périphériques en compromettant leurs infrastructures et équipements informatiques (réseaux, pare-feu, routeurs…) pour y implémenter des accès discrets de type *portes dérobées*, voire des implants logiciels pré-positionnés à l'instar d'une *cinquième colonne numérique* : prestataires, fournisseurs, sous-traitants, organismes de tutelle, chaine d'approvisionnement, etc. Du fait d'une intégration technique toujours plus poussée, l'espace numérique favorise des phénomènes et des risques de nature systémique. Ainsi, confrontée à l'espionnage, au sabotage et à la déstabilisation, la France tente de se protéger voire de contre-attaquer. Pourtant, malgré une législation et des politiques publiques empilées et renforcées[6], le pays accuse le coup comme en témoignent les régulières unes médiatiques sur le sujet.

Comment, dès lors, expliquer l'apparente impuissance à enrayer ces attaques informatiques et informationnelles ? La France utilise-t-elle tous les moyens et ressources en sa possession ? C'est ce questionnement qui a constitué le point de départ de notre recherche. Avec l'intuition initiale qu'un acteur pourtant central du cyberespace était éludé alors qu'il constitue possiblement le chainon manquant de la cybersécurité nationale. Cet acteur, c'est précisément ce profil atypique, ce hacker qui est l'objet de tant de fantasmes et de stéréotypes. Fascinante et repoussante à la fois, la figure du hacker a progressivement été réhabilitée

[3] https://www.blogdumoderateur.com/bilan-cyberattaques-pme-les-plus-exposees/.
[4] Les *ransomwares*/rançongiciels sont des logiciels malveillants (maliciels/*malwares*).
[5] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
[6] Entre autres : https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ ; http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf.

ailleurs[7] et très certainement rejugée avec précaution et récemment en France. C'est que la culture hacker s'implémente mal dans notre *stratologie* – logiciel stratégique – nationale. En effet, si un type particulier de hackers, le hacker dit « éthique » est aujourd'hui l'objet de toutes les attentions voire de convoitises et le sujet d'un large traitement médiatique, le soupçon à son endroit semble néanmoins rester chevillé au corps politico-économique.

Précisément, au moment où nous débutions cette thèse, en 2016, une *Loi pour la République numérique*[8] venait indirectement et mollement autoriser, plus que le reconnaître, le hacking éthique en France. C'est, en effet, par le truchement du déjà fragile à l'époque statut de lanceur d'alerte que la notion de *lanceur d'alerte de sécurité* puis plus tard de *lanceur d'alerte numérique* a été admise[9]. Dans un cadre légal strict, les hackers pouvaient alors assurer des prestations d'audit en « cybersécurité offensive », concept toutefois encore peu usité et plus volontiers reconnu aux États-Unis d'Amérique (EUA*). Au fil de notre travail, nous avons vu monter en puissance la figure du hacker éthique. Par appétence, curiosité tous azimuts et contact précoce avec l'outil informatique, nous nous sommes rapproché du monde du hacking pour compléter nos connaissances en chantier permanent sur la cybersécurité. Car la nécessité toute socratique que l'on sait qu'on ne sait rien se traduit aussi dans le code des hackers ; que l'on soit de l'équipe rouge ou de la bleue[10], la connaissance est une quête sans fin. Ce principe, qui a toujours été intimement le nôtre trouvait écho dans la formule du hacker Éric S. Raymond : « *Crois en ta capacité à apprendre*.[11] » Profil un peu atypique nous-même, sillonnant diverses contrées du savoir principalement dans le cadre de notre activité d'enseignant, traversée de quelques séquences comme consultant et réserviste[12], entre histoire, géopolitique et intelligence économique, notre objectif a consisté à mieux appréhender le monde du hacking. Nous avons ainsi souhaité nous positionner à l'intersection du monde académique et du monde pratique en nous formant à l'une des activités les plus développées chez les hackers, le *pentesting*. Ce faisant, notre humble immersion dans le milieu du hacking nous a ouvert les portes d'un monde arrimé au réel, où la franchise et l'accessibilité de ses protagonistes ont été l'objet d'un certain étonnement initial. Dans la lignée de l'éthique hacker, nous saisissâmes rapidement les mots de Steven Levy : « *Un hacker ne doit pas être jugé sur*

[7] Pekka Himanen, *L'éthique hacker et l'esprit de l'ère de l'information*, Exils, 2001 ; Steven Levy, *Hackers: Heroes of the Computer Revolution*, Doubleday, 1984, trad. en français : *L'Éthique des hackers*, Globe, 2013, 528 p.
[8] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/
[9] Les deux notions sont équivalentes et dénotent les tâtonnements à bien définir le statut d'un lanceur d'alerte signalant des failles de sécurité numérique.
[10] *Red team (attaquants)* / *Blue team (défenseurs)*. Nous reviendrons sur ces notions.
[11] Samuel Verley & Élodie Perrotin, *Qui sont les hackers ?*, Éd. du Ricochet, 2018, 128 p., p. 26.
[12] Nous avons été pendant trois ans réserviste opérationnel-spécialiste pour le CRR-FR de Lille (OTAN France) et depuis cinq ans réserviste citoyen de gendarmerie et de cyberdéfense (R*éserve C*itoyenne de C*yberdéfense*).

*ce qu'il est, mais sur ce qu'il fait*.[13] » C'est en les côtoyant que nous avons pu nourrir notre réflexion dans une dynamique de va-et-vient entre empirie et théorie.

Deux ans plus tard, en 2018, la ministre des Armées, Florence Parly, dévoilait un pan de la doctrine d'emploi de lutte informatique offensive (LIO)[14] en officialisant le fait que la France se donnait le droit d'user de cyberattaques dans le cadre d'opérations militaires. Dans ce sillage, évoquant les questions de recrutement liées aux besoins de la Loi de programmation militaire, Mme Parly préconisait d'ouvrir ce dernier à des profils atypiques, sans véritablement préciser ni désigner les hackers. Si le positionnement est louable, ces annonces ont-elles pour autant été suivies d'effet, alors que la ministre pointait encore en 2020 les difficultés de la France à recruter de tels profils notamment dans l'Armée ?[15]

* * *

Ainsi, les hackers ont-ils depuis été approchés, sollicités, recrutés, par l'Armée, par la société civile ? D'ailleurs, l'enjeu de la cybersécurité se limite-t-il à la seule cyberdéfense ? En d'autres termes, la cybersécurité est-elle seulement une affaire de militaires ? Surtout, si des hackers sont recrutés, quelle est la nature réelle de cette collaboration ? À notre connaissance et dans l'état de l'art scientifique, il s'avère que cette question n'a jamais été traitée en France ni même directement aux États-Unis où pourtant l'emploi régulier de hackers est attesté, notamment au sein des services de renseignement. La raison en est que les hackers sont généralement appréhendés soit comme des pirates informatiques, à l'aune de leur philosophie singulière ou encore par le prisme sociologique/anthropologique des différentes communautés historiques qu'ils ont fondées ou autour desquelles ils gravitent. Du reste, c'est souvent un certain étonnement, cette fois de la part de nos interlocuteurs hackers, qui se faisait jour à l'entame de nos entretiens, lorsqu'ils se voyaient interrogés sur leurs rapports avec notamment les autorités. Ce qui démontre que le sujet ne leur a jamais été exposé, y compris de la part de journalistes spécialisés[16].

Par conséquent, il nous a paru nécessaire de questionner les liens qu'entretenaient en France l'État et les entreprises avec les hackers, en vue de juger du degré de synergie qui les unirait dans le cadre de la stratégie de sécurité numérique. De là découle la problématique suivante :

[13] Steven Levy, *Hackers: Heroes of the Computer Revolution*, *ibid*.
[14] https://www.defense.gouv.fr/sites/default/files/ministere-armees/Lutte%20informatique%20offensive%20%28LIO%29.PDF
[15] https://www.liberation.fr/france/2020/07/13/la-diversite-est-tres-faible-dans-les-grandes-ecoles-militaires_1794108/
[16] Parmi eux, Jean-Marc Manach – que nous avons interviewé –, tout en travaillant sur le monde des TIC, de l'investigation numérique et du cyber, n'a pas directement adopté cet angle.

Les sphères politique et économique (autorités étatiques/entreprises) entretiennent-elles avec les hackers des rapports à même de favoriser l'émergence d'un dispositif intelligent dans le cadre d'une stratégie de cybersécurité nationale ?

Ainsi, ce travail de recherche vise à sonder le niveau d'intégration des hackers dans les politiques de sécurité en analysant la nature de cette relation. Ces acteurs communiquent-ils réellement ? En somme, sont-ils placés dans une dynamique de stratégie-réseau ?

* * *

Pour ce faire, nous avons pris le parti d'emprunter une voie plutôt rare en science. Ainsi, une approche abductive a été adoptée dans le cadre de notre démarche de recherche. Parmi les trois types d'inférence logique qui font l'objet du consensus scientifique, entre induction et déduction, l'abduction tient une place marginale. Cette démarche, qui s'inscrit dans la théorie pragmatiste – entre constructivisme et positivisme –, permet d'élaborer une connaissance probable ou possible, et peut se révéler utile si l'on souhaite éviter l'écueil de la démonstration péremptoire[17]. Or, eu égard à la difficulté inhérente à nos objet et sujet de recherche, cette démarche nous a semblé tout à fait pertinente. À l'image d'une boucle récursive (dite ADI)[18], l'abduction permet en effet, partant de données empiriques et d'observations (phase abductive-A), de formuler des hypothèses (phase déductive-D), de les vérifier pour mettre au jour des théories (phase inductive-I), lesquelles sont soumises ensuite aux données de départ. Pour Javier Nuñez Moscoso, c'est un exercice intellectuel dual, une opération paradoxale « *d'instinct rationnel* », entre création et argumentation scientifiques[19]. Ainsi, nous faisons nôtre en la paraphrasant la formule de l'historien Lucien Febvre selon qui « *le scientifique ne trouve pas, il cherche*. »

D'un point de vue méthodologique, une approche qualitative et réflexiviste déclinée en deux axes a été adoptée en vue de faire émerger des données par nature assez délicates à obtenir. D'une part, des entretiens ont été réalisés auprès de plusieurs experts, d'autre part nous avons procédé à quatre études de cas afin de tester nos hypothèses de travail.
La démarche similaire suivie dans le cadre de nos travaux précédents – notamment en Relations internationales –, qui portaient sur le renseignement et son influence, nous a encouragé à penser qu'en dépit des difficultés à collecter des informations souvent

[17] Yves Hallée & Julie M. É. Garneau, « L'abduction comme mode d'inférence et méthode de recherche : de l'origine à aujourd'hui », *Recherches qualitatives*, 38(1), 2019, pp. 124–140.
[18] Voir schéma en partie 3, chapitre 6, p. 328.
[19] Javier Nuñez Moscoso, « Et si l'on osait une épistémologie de la découverte ? La démarche abductive au service de l'analyse du travail enseignant », *Penser l'éducation*, 33, 2013, pp. 57-80.

confidentielles ou grises propres à ces domaines, possibilité nous était donnée de parvenir à des résultats exploitables. C'est ce fil conducteur qui a présidé à la méthode qualitative de l'entretien individuel ici appliquée, couplée à l'observation si ce n'est *in situ* du moins de proximité avec le milieu étudié (l'immersion précitée), à l'interface entre services de sécurité et profils de hackers. Trente-cinq entretiens ont été réalisés auprès d'acteurs issus ou placés au carrefour des trois sphères étudiées : économique, politico-sécuritaire et celle des hackers. On trouvera le verbatim de ces entretiens ouverts en annexes. Le deuxième axe de notre méthodologie, par ailleurs nourri du premier, a consisté à réaliser quatre étude de cas propres à éclairer notre entreprise.

La mise en œuvre de ce travail de recherche s'articule ainsi sur trois partie. La première consiste tout d'abord en un état des lieux général des politiques publiques de sécurité numérique en France. Nous questionnons et caractérisons en premier point la notion de cyberespace, afin de mieux comprendre la manière dont l'État français appréhende ce milieu et les menaces qu'il génère dans le cadre d'une stratégie de cybersécurité. Il s'agit en effet d'apprécier comment et avec quelles ressources les autorités gèrent les attaques informationnelles au sens large. En second lieu, après avoir constaté que les hackers ne font pas partie intégrante de cette stratégie nationale, nous étudions leur univers, leurs éthique et culture pour mieux expliquer la méfiance dont ils font très largement l'objet. Au-delà des fantasmes et poncifs convenus, qui sont véritablement les hackers ? Forment-ils une communauté unique et unie ? Servent-ils des intérêts égoïstes ou font-ils montre de patriotisme ? En quoi constitueraient-ils, dès lors, un atout pour le pays ?

Pour répondre à ces interrogations et saisir pourquoi les mondes politique et économique ne considèrent pas naturellement les hackers comme un avantage, il est nécessaire de dévoiler la toile de fond qui sert de trame à la cybermenace mondiale. C'est l'objet de la deuxième partie de ce travail qui se donne pour objectif d'analyser les enjeux et défis du cyber par le prisme de l'intelligence économique (IE*). Ainsi, dans un premier temps, nous mettons en exergue l'un des courants de la discipline les plus représentés en France à travers le postulat de la *guerre économique*, approche littéralement polémique mais résolument pragmatique des rapports de puissance qui structurent l'ordre international. Nous proposons en outre de le dépasser pour évoquer le concept de *guerre systémique*, lequel fait écho à la vision stratégique du Chef d'état-major des Armées (2021). Puis, nous convoquons l'intelligence économique, que nous définissons et caractérisons en vue de modéliser une grille de lecture pertinente pour appréhender l'un des pans de cette conflictualité holistique, déclinée dans l'espace numérique en une *cyberguerre*. Cette notion elle aussi controversée fera l'objet d'une illustration à travers une supra-analyse mettant en exergue le rôle joué par le hacking dans les guerres informationnelles.

Enfin, une dernière partie viendra, dans un premier temps, opérationnaliser notre modèle théorique appliqué à quatre études de cas. Cette charnière greffant IE et cyber sera utile pour soumettre à la grille de lecture ces cas pratiques choisis pour leur représentativité mais aussi contraints par le manque de sources disponibles liées à notre sujet. Dans un second temps est proposé et défini le concept d'*Intelligence cyber*, que nous avons forgé en l'adossant à celui d'intelligence économique. La cyberconflictualité et les guerres informationnelles s'inscrivant dans ce que nous appelons la *guerre systémique*[20], de fait le croisement avec l'IE s'avère pertinent. Enfin, dans un troisième temps, nous formulons des préconisations pour la mise en œuvre de l'intelligence cyber. Celle-ci se conçoit comme une boussole stratégique pour fixer un cap et suivre un horizon. Car, comme nous le rappelle Sénèque, « *Il n'est pas de vent favorable à celui qui ne sait où il va*. » Ainsi, nous recommandons, d'une part, d'élaborer une politique nationale d'intelligence cyber dotée notamment d'un volet éducatif développé et visant à élever le niveau général de culture du renseignement et de cybersécurité. D'autre part, d'arrimer les hackers patriotes qui sont forces de propositions dans un dispositif de défense des intérêts de la France dans le cyberespace, à l'image de Marc Sejean, Florent Curtet ou Alexandre Oda, lesquels seront présentés dans le corps de ce travail. Ces hackers pourraient dès lors axer leur action sur trois piliers inspirés de l'intelligence économique : renseignement ouvert, cybersécurité offensive et cyber-influence. Dans cette perspective, partant du constat que les hackers les plus compétents sont des profils parfois hors cadre, la création d'une interface de dialogue formelle pourrait se révéler profitable pour tisser un rapport de confiance avec les institutions et autorités étatiques.

En définitive, il s'agit d'avoir à l'esprit que dans un contexte de compétition globale, une posture offensive est plus que jamais impérieuse sinon nécessaire à adopter en vue d'établir un véritable État-cyberstratège. Pour que le pays ne subisse plus mais le dispute agilement face aux autres puissances.

[20] Nous expliciterons plus loin cette notion.

# I. La cybersécurité nationale et les hackers

# Chapitre 1 | Cyberespace et cybersécurité

> « *Le cyberspace. Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques… Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumière disposés dans le non-espace de l'esprit, des amas et des constellations de données. Comme les lumières de villes, dans le lointain…* »
>
> William Gibson (*Neuromancien*)

Pour paraphraser tout à la fois Raymond Aron et Pierre Hassner, l'on pourrait avancer que la cyberpaix est impossible et la cyberguerre un peu moins improbable. C'est que le cyberespace fait l'objet d'une mythification au même titre qu'une mystification. Imaginé par Platon, rêvé par Teilhard de Chardin en *noosphère* interconnectant l'ensemble des psychés humaines, le cyberespace et en particulier l'Internet a été vu d'abord comme l'avènement d'un *village global* maillé « d'autoroutes de l'information », puis tel un monde anxiogène regorgeant de menaces. Passant d'un extrême à l'autre, le regard posé sur cet artefact soumet la réflexion à un tumulte incessant du fait même de l'instabilité de cette *hyperstructure*. *Web*, *cloud*, *virus*, *dorsale* ; *milieu*, *domaine*, *espace*… autant d'expressions imagées et d'hésitations sémantiques qui témoignent d'une nécessité analogicienne et relèvent de puissantes représentations typiques d'une difficulté à appréhender cet environnement complexe. Nous façonnons le cyberespace qui nous façonne à son tour.

Indissociable d'aspects techniques et d'une dimension sociopolitique, le domaine numérique porte en lui des enjeux de pouvoirs et donc par extension de sécurité, celle des réseaux informatiques, des langages logiciels mais aussi des rapports humains et internationaux. Dans cette optique, l'État français a pris des mesures et déployé des politiques de cybersécurité qui ont été renforcées et clarifiées à partir de 2008 et surtout 2013 avec la publication des Livres blancs de défense et de sécurité nationale (LBDSN). Parmi cette série de dispositions juridiques, le sous-domaine de la cyberdéfense cristallise les attentions et se focalise sur les aspects techniques de la sécurité numérique. En 2018, les autorités révèlent officiellement procéder à des cyberattaques dans le cadre d'une doctrine de lutte informatique offensive (LIO). Couplée avec son volet défensif (LID) et celui, tardif, d'une lutte d'influence (L2I), cette politique semble aujourd'hui atteindre une certaine maturité. Toutefois, la présence prééminente d'acteurs étatiques notamment militaires dans ce dispositif semble occulter les acteurs privés, dénotant un manque d'intégration et une réelle stratégie de cybersécurité globale. Tout particulièrement, les *hackers* sont absents des débats autour de la sécurité numérique alors qu'ils tiennent un rôle de plus en plus incontournable comme utilisateurs, producteurs, protecteurs et innovateurs du cyberespace.

## **A.** *Enjeux de la sécurité numérique*

La numérisation globalisée engendre un niveau d'interdépendance et d'interconnexion inédit des sociétés humaines. Cet enchevêtrement d'acteurs et d'intérêts disparates forme le premier vivier de la cybermenace. Cette mise en réseaux des activités humaines revêt en effet un caractère systémique où les centres et hiérarchies traditionnels du pouvoir s'estompent et cèdent le pas à une horizontalisation des rapports entre les parties prenantes. De la criminalité appliquée au cyberespace à la cyberguerre, en passant par le cyberterrorisme ou le cyber-renseignement, tous les champs d'activités sont augmentés dans une *datasphère*[21] qui fait l'objet de multiples convoitises. Extraction ou collecte légale puis revente de données personnelles, espionnage des communications et surveillance de la navigation internautique, altération des systèmes informatisés voire sabotage des câbles optiques, détournement de flux financiers, piratage de systèmes embarqués ou d'objets connectés, défacement de sites web et *phishing*, usurpation d'identité et *doxxing*[22], viol des messageries électroniques… Cette longue liste pourtant non exhaustive donne une idée de l'étendue de la surface d'attaque qu'exploitent des cybercriminels bien sûr, mais aussi parfois des acteurs légitimes. Acteurs politiques et parfois privés qui achètent ou commercialisent des solutions de surveillance et d'espionnage ainsi que des vulnérabilités logicielles ; acteurs économiques se rémunérant par les capitalisation, corrélation et vente des données privées d'usagers dont on obtient le consentement plus ou moins éclairé.

Précisément, dix ans après les révélations publiques du lanceur d'alerte Edward Snowden[23], la question de la confidentialité en ligne et en particulier de la vie privée sur les réseaux socionumériques (RSN*) a fait long feu. En dépit de législations européennes volontaristes visant à encadrer la collecte massive de données à caractère privé (DCP), les « géants du numérique » continuent de vouloir contourner ces limitations ou exploitent la naïveté et la négligence des utilisateurs, particuliers ou entreprises. Or, la *privacy* comme on la désigne en pays anglosaxon est indissociable de la cybersécurité. La *confidentialité* constitue

[21] Concept utilisé par l'école française de géopolitique représentée par l'IFG de l'université Paris 8. Voir « Géopolitique de la datasphère », *Hérodote* 2020/2-3 (N° 177-178), La Découverte, 2020, 384 p. L'expression « sphère des données » est empruntée à Jean-Sylvestre Bergé & Stéphane Grumbach, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », *Journal du droit international,* Clunet, n° 4, Octobre 2016, var. 6.

[22] Le *doxxing* est la recherche puis la divulgation de données personnelles et informations privées d'un internaute dans le but de nuire à sa réputation. Voir par exemple : https://www.lesnumeriques.com/vie-du-net/qu-est-ce-que-le-doxxing-et-pourquoi-est-il-desormais-puni-par-la-loi-a168491.html. Pour des exemples sur les autres atteintes, voir notamment Nicolas Arpagian, *La cybersécurité*, coll. « Que sais-je ? », PUF, 2022, 128 p.

[23] Rappelons qu'Edward Snowden a divulgué en 2013 des informations classifiées sur les programmes de surveillance de masse mis en place par la *National Security Agency* (NSA) pour laquelle il travaillait comme sous-traitant. On peut notamment citer le programme *PRISM* qui imposait aux sociétés numériques américaines de livrer les données de leurs utilisateurs sur simple demande de l'État.

d'ailleurs le premier pilier d'une triade à préserver dans une politique de sécurité des systèmes d'information, avec l'*intégrité* et la *disponibilité* auxquelles on ajoute parfois l'*authenticité*[24]. C'est donc l'un des principaux enjeux de la cybersécurité et suppose par conséquent un fort degré de souveraineté numérique. Inscrites dans la droite ligne du principe d'« autonomie stratégique »[25], les politiques de cybersécurité nationale et leur déclinaison de cyberdéfense sont pourtant le résultat de choix contradictoires qui ont trait à l'inconfort d'une dépendance technologique subie de longue date. Les atermoiements manifestes du positionnement de l'État français témoignent d'une difficulté à prendre en main son propre destin technologique en association avec ses partenaires européens. Ainsi, en 2018, la Revue nationale de cyberdéfense fait prévaloir une *autonomie stratégique numérique*, jugée plus consensuelle et réaliste selon Alix Desforges[26]. Tandis qu'en 2021 est initiée une Mission d'information sur la souveraineté numérique nationale et européenne qui consacre de nouveau l'idée d'une vraie reprise en main de l'État[27]. La première forme de cybersécurité est donc vraisemblablement liée à un encerclement cognitif ou une résignation face à des cyberpuissances comme les États-Unis ou la Chine.

La notion d'encerclement ou plus globalement de *guerre cognitive* – qui sera développée plus loin – se rapporte aux stratégies couvertes ou ouvertes de domination par le modèlement de l'univers mental des adversaires, en agissant sur leur environnement pour les influencer indirectement. « *Ainsi se forme un écheveau de dépendances invisibles qui forme le cœur des stratégies de puissance contemporaines*.[28] » résume Raphaël Chauvancy. Cette guerre se fait par le *contenant* et le *contenu*, via le vecteur et l'information, autrement dit les infrastructures transportant la donnée et l'instrumentalisation de la donnée elle-même. Ainsi est-il nécessaire de comprendre ce qu'est précisément le cyberespace puisqu'il combine ces deux dimensions désormais inextricablement mêlées dans un champ informationnel systémique.

[24] La *confidentialité* suppose de toute information/donnée qu'elle soit soumise à un « besoin d'en connaître » autorisé à des personnes identifiées ; son corollaire, le principe d'*authenticité*, repose sur une vérification de l'identité de ces mêmes bénéficiaires ; l'*intégrité* suppose l'interdiction d'altérer cette information ; la *disponibilité* enfin renvoie à la possibilité d'un accès continu à ladite information/donnée.

[25] D'une manière générale, l'autonomie stratégique peut être comprise comme la capacité pour un État ou un groupe d'États de disposer d'une liberté d'appréciation, de jugement et d'action dans divers domaines : défense, économie, énergie, technologie. Elle est intiment liée à la notion de souveraineté.

[26] Alix Desforges, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques » in Géopolitique de la datasphère, *Hérodote*, *op. cit.*, pp. 179-195.

[27] https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information#_Toc256000143

[28] https://geopoweb.fr/?LES-NOUVELLES-GUERRES-SYSTEMIQUES-NON-MILITAIRES-Par-Raphael-CHAUVANCY

## **1)** Définition et représentations du cyberespace

> « *Frontières : en géographie politique, ligne imaginaire entre deux nations, séparant les droits imaginaires de l'une des droits imaginaires de l'autre*. »
>
> Ambrose Bierce (*Devil's Dictionnary*)

Si tout le monde parle « du cyber » par convention et habitude, il est toutefois malaisé de définir avec précision cet objet d'étude flou aux contours incertains que l'on peut désigner par plus d'une dizaine de qualificatifs jamais pleinement satisfaisants. Ainsi, le grand public l'assimile à l'Internet, un « réseau de réseaux » mondial sur lequel on peut naviguer sur des « sites internet », par ailleurs lui-même confondu le plus clair du temps avec le *World Wide Web* qui n'en est qu'une application. Assimilé à une toile virtuelle, le Web est un système fondé sur des liens hypertextes qui relient entre elles des pages/informations contenant des ressources multimédias par le biais de l'Internet qui sert de réceptacle et véhicule physiques. Créé en 1989, le Web est comme un réseau virtuel sur lequel on évolue grâce à des logiciels appelés « navigateurs », l'Internet étant quant à lui le réseau matériel permettant de stocker et mobiliser l'information – dont les sites web – sur des serveurs, à savoir des ordinateurs interconnectés par des réseaux informatiques recoupés par des équipements d'aiguillage (routeurs, commutateurs, IXP…[29]). Ces serveurs sont des dispositifs matériels et logiciels qui sont largement dédiés aujourd'hui à l'hébergement de sites web et offrent des services à des utilisateurs dits « clients ». Ce dialogue client/serveur constitue un modèle informatique qui assure aujourd'hui le fonctionnement privilégié de la communication entre ordinateurs. Ces serveurs peuvent néanmoins avoir d'autres applications, comme la prise en charge des stockage et acheminement du courrier électronique, dont les serveurs spécifiques sont désignés par l'appellation *Mail eXchanger* (MX)[30].

Définir le cyberespace n'est pas chose aisée. Nous présentons ci-dessous quelques propositions élémentaires principalement françaises et faisant autorité.

[29] Un routeur est un équipement chargé d'aiguiller les paquets IP (*Internet protocol*, via des adresses logiques) de données entre interfaces réseau. Subséquemment, un commutateur réseau (*switch*) est un équipement acheminant des trames (via des adresses physiques) notamment aux machines d'un réseau local (LAN). Un *Internet eXchange Point* (IXP) est une interface infrastructurelle physique permettant de relier des systèmes autonomes (AS) gérés par des fournisseurs d'accès à l'Internet à travers des accords de « peering ». Les systèmes autonomes sont des ensembles de réseaux informatiques unifiés par une grande interopérabilité et des politiques (protocoles de communication) de routage cohérentes.

[30] Beaucoup de serveurs de messagerie électronique, qui auparavant nécessitaient un client de messagerie (un logiciel en local), sont toutefois incorporés aujourd'hui dans le web, ce qu'on appelle des *webmails*.

***Définitions liminaires du cyberespace***

Partons des dictionnaires usuels français. En premier lieu, le Robert propose : « *Espace de communication créé par l'interconnexion mondiale des ordinateurs (internet) et par les données qui y sont traitées ; espace, milieu dans lequel naviguent les internautes.* »

La définition de l'ANSSI, datée de 2011, est quasi identique : « *Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.*[31] »

Voici la notice *cyberespace* du Petit Robert en 2015 : « *Ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.*[32] »

Le Larousse, enfin : « *Espace virtuel rassemblant la communauté des internautes et les ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs.* »

« *L'environnement complexe résultant de l'interaction de personnes, de logiciels et de services sur l'Internet au moyen de dispositifs technologiques et de réseaux qui y sont connectés, et qui n'existe sous aucune forme physique.* » (NIST/DoC)[33]

À ce stade, il est intéressant de noter que ces définitions portent essentiellement sur des aspects techniques, liés aux équipements informatiques. Toutefois, le Robert aborde des aspects plus immatériels et sociétaux, évoquant des « ressources d'information », un espace « virtuel », et une « communauté ». Sa définition en 2015 est plus significative encore avec des mentions comme « univers d'information » ou « milieu ». De même, prolongeant cette logique, la proposition du NIST aborde plus distinctement les dimensions logicielles, humaines et sociales du cyberespace, quitte cette fois à minimiser ses aspects techniques.

[31] https://www.ssi.gouv.fr/entreprise/glossaire/c/

[32] Astrid Kempf, « Pour une sociologie du cyberespace », *Revue Défense Nationale*, 2015/10 (N° 785), pp. 77-82.

[33] https://csrc.nist.gov/glossary/term/cyberspace. Cette définition est issue d'un document produit par une agence du Département du Commerce américain, le NIST (National Institute of Standards and Technology).

***Définitions militaires du cyberespace***

« *Le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne.* »

Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE, 2011)[34]

« *Le cyberespace est le réseau planétaire qui relie virtuellement les activités humaines grâce à l'interconnexion des ordinateurs et permet la circulation et l'échange rapides d'informations.* » CICDE (Concept d'emploi des forces, janvier 2010)[35]

« *Un domaine global situé dans l'environnement de l'information et constitué d'un réseau interdépendant d'infrastructures, de technologies et systèmes d'information, incluant l'Internet, les réseaux de télécommunications, les systèmes informatiques et les processeurs et contrôleurs intégrés.* » Département de la Défense américain (DoD)[36]

On constate ici des aspects disparates, qui ont trait à l'approche pratique et donc technique de la réflexion militaire, mais aussi à des éléments plus abstraits qui renvoient à une dimension immatérielle. L'approche américaine met l'accent sur le champ informationnel, suggérant une subordination des aspects techniques à celui-ci – même si l'information peut avoir la double acception. La Russie, par ailleurs, fait de même avec plus de clarté du reste, puisqu'elle évoque ouvertement « l'espace informationnel » en le substituant au concept de cyberespace plus occidental, et parle volontiers de « souveraineté informationnelle »[37]. Dans un régime autocratique comme la Russie où il est vital d'en avoir le contrôle, l'information concerne tout autant des enjeux de politique intérieure que de politique étrangère. Les guerres de l'information et le *sharp power*[38] peuvent ainsi se déployer dans ce champ où manipulations

[34] Cité par Delphine Deschaux-Dutard (dir.), « Cybersécurité internationale », *Introduction à la sécurité internationale*, PUG, 2018, pp. 209-225.
[35] *Idem*.
[36] https://csrc.nist.gov/glossary/term/cyberspace
[37] Maxime Audinet et Céline Marangé, « La Russie : "l'espace informationnel" comme terrain de conflictualité », *Les guerres de l'information à l'ère numérique*, PUF, 2021, pp. 115-136. La doctrine Gerasimov de « guerre nouvelle génération » publiée en 2014 est éclairante à ce sujet. Voir par exemple : https://www.frstrategie.org/programmes/observatoire-armee-de-terre-2035/concept-russe-guerre-nouvelle-generation-general-gerasimov-quelle-exploitation-pour-armee-terre-2020 ou encore : https://www.portail-ie.fr/univers/defense-industrie-de-larmement-et-renseignement/2022/guerre-hybride-et-sharp-power-du-kosovo-a-lukraine-construction-dune-nouvelle-strategie-politico-militaire-russe-a-lere-gerasimov-partie-1-2/
[38] Le *sharp power* est une notion inventée par deux chercheurs du *think tank* américain National Endowment for Democracy (NED) pour désigner la puissance « tranchante » dont usent les régimes autoritaires à l'encontre des démocraties libérales. Cette modalité de puissance est le miroir inversé du *soft power* cherchant à « gagner le cœur et les esprits », et vise ainsi à « déchirer » le contrat social des pays occidentaux, leur environnement

des contenus et influence narrative d'une part, attaques informatiques d'autre part se greffent à des moyens militaires plus traditionnels.

Au bilan, ces définitions ne semblent pas englober toute la complexité du concept, en le restreignant notamment à des éléments techniques ou, quand elles le font, en disjoignant les trois vraisemblables dimensions (matérialité, immatérialité, humanité).

***Apports complémentaires***

« *Le cyberespace se définit comme le maillage des réseaux permettant l'interconnexion informationnelle des êtres vivants et des machines*.[39] » Stéphane Dossé & Olivier Kempf

Cette définition, qui a le mérite d'être concise et nous rapproche de ces trois dimensions, n'évoque toutefois pas explicitement l'aspect logique-logiciel.

« *Le cyberespace est une dimension duale, physique et logique : le lieu de l'interaction entre le maillage des réseaux de communications et les données qui y transitent*.[40] » Anonyme

Cette définition intéressante et prenant en compte justement l'aspect logique remise toutefois la dimension humaine. Elle comporte l'idée pertinente de superposer au réseau physique un réseau logique, mais oublie le(s) réseau(x) humain(s). Le cyberespace se déploie bien sur trois dimensions et non seulement deux.

« *La datasphère peut se concevoir comme la représentation d'un nouvel ensemble spatial formé par la totalité des données numériques et des technologies qui la sous-tendent, ainsi que de leurs interactions avec le monde physique, humain et politique dans lequel elle est ancrée*.[41] »

La notion de datasphère de Frédérick Douzet est reprise des travaux de Stéphane Grumbach et Jean-Sylvestre Bergé fondés sur l'approche controversée d'une géologie de l'anthropocène. Frédérick Douzet propose de la substituer au concept de cyberespace. Quoique sa pertinence ne fasse pas de doute d'un certain point de vue, nous pensons toutefois que la

politique et informationnel par des pratiques de subversion, menaces latentes, coercition, auto-censure, dans une sorte d'*effet Golem* généralisé à une population et ses valeurs-clés (légitimité démocratique, primauté du droit sur la force, libertés individuelles...)

[39] Stéphane Dossé & Olivier Kempf (dir.), « Les principes stratégiques du milieu cyber », *in* Stratégies dans le cyberespace, *Cahiers de l'alliance géostratégique* (n°2), L'esprit du livre, 2011, 210 p., pp. 181-188.

[40] Cité par un bloggeur anonyme : https://web.archive.org/web/20131220045408/http://cyber-defense.fr/blog/index.php?post/2012-01-15/Bienvenue-sur-Dotclear%C2%A0%21

[41] Frédérick Douzet, « Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique », *Hérodote*, 2020/2-3 (N° 177-178), pp. 3-15.

notion ne prend pas plus ni mieux la pleine mesure du concept originel de cyberespace et induit une apparente simplification – certes utile – ou une fausse clarification[42].

Par conséquent, nous soutenons que le concept de cyberespace reste valide, qu'il est aussi voire plus pertinent et rend compte au mieux, et à défaut de traduire toute la complexité du phénomène, de la réalité de l'entité qu'il constitue. Certes, les données de flux apportent une épaisseur[43] à l'objet étudié et amène sa vulgarisation par une approche cartographique, mais *la carte n'est pas le territoire*. La donnée est fondamentale, mais l'humain reste au centre de l'objet et de l'enjeu. On assiste bien à la « mise en données » du monde, mais surtout à sa mise en réseaux. Car, ainsi que le retrace Armand Mattelart, *« de multiples acteurs, publics et privés, ont contribué à dessiner la topographie des réseaux et des systèmes à l'échelle mondiale. Ils l'ont fait en invoquant des idéaux et motivés par les intérêts les plus divers : l'universalisme d'une civilisation prédestinée, l'œcuménisme d'une religion, l'interdépendance des nations commandée par la sécurité mutuelle, le pragmatisme de l'entreprise et l'impératif catégorique de la division internationale du travail ou encore la communauté de lutte des opprimés. Figure maîtresse du progrès, l'univers réticulaire a aussi investi les utopies. Éternelle promesse, le réseau de communication symbolise la figure d'un monde meilleur parce que solidaire. De la route au rail jusqu'aux "autoroutes de l'information", cette croyance a rebondi au gré des générations techniques. Mais les réseaux n'ont jamais cessé d'être au centre des luttes pour la maîtrise du monde.*[44] »

« *Définir*, nous dit Samuel Butler, *c'est entourer d'un mur de mots un terrain vague d'idées*. » Mais c'est aussi donner à comprendre ou à réfléchir. Nous proposons donc ici une définition-synthèse sans prétention, qui viendra peut-être apporter une nouvelle *donnée* à la difficile équation du décryptage du phénomène.

[42] En effet, d'une part, elle se base sur une analogie du concept géographique d'hydrosphère, d'autre part ce biais précisément géographique est certes consensuellement convoqué mais reste une métaphore du territoire ou d'un espace physique – même s'il est question d'une « représentation ». Par ailleurs, la notion de donnée renvoie bien plus à des aspects techniques et logiciels, mais pas vraiment à une dimension cognitive et humaine, sauf à considérer par projection temporelle et logique transhumaniste que l'humain soit résumé à un objet numérique en soi. C'est ce qu'évoque du reste l'autrice en évoquant les questions algorithmiques et d'intelligence artificielle. Cette approche « datacentrée » semble, au bout du compte, trop neutre alors que la donnée numérique ne l'est pas. La donnée n'est justement pas *donnée*.

[43] https://web.archive.org/web/20131220045408/http://cyber-defense.fr/blog/index.php?post/2012-01-15/Bienvenue-sur-Dotclear%C2%A0%21

[44] Armand Mattelart, *La mondialisation de la communication*, PUF – Que sais-je ?, 1996, pp. 3-4.

***Essai de définition-synthèse***

*Le cyberespace est un artefact trilogique virtuellement territorialisé et physiquement matérialisé. Il forme un espace réticulé de communication généré par l'interconnexion de trois réseaux informationnels, alimentés par la circulation de données numériques : un réseau physique (maillage informatique dont l'Internet), un réseau logique (maillage applicatif du code) et un réseau sociocognitif (maillage interactionnel humain).*

Pour résumer, le cyberespace représente l'intrication d'objets physiques (l'Internet et autres réseaux de télécommunication, systèmes autonomes) avec des ressources logiques (interface articulant matériel et immatériel par le langage machine/informatique) et sémantiques (le Web et ses applications). C'est sa complexité intrinsèque, liée d'abord à des infrastructures certes mesurables mais relativement opaques, puis associée à l'idée d'une immatérialité abstraite qui confère au cyberespace tout son mystère. Pourtant, le concept s'est imposé pour devenir relativement consensuel et l'objet d'une appropriation stratégique tant de la part des acteurs privés pour des raisons lucratives ou de contestation sociétale et de mobilisation idéologique que des États à des fins politiques et militaires.

**a) *Le cyberespace, objet de représentations rivales***

Deux principales visions de l'espace numérique s'opposent : la première est celle des pionniers de l'Internet consacrée par la formule restée célèbre de feu John P. Barlow, militant libertaire cofondateur de l'ONG Electronic Frontier Foundation et par ailleurs membre historique du groupe de rock Grateful Dead. Issue de la *Déclaration d'indépendance du cyberespace* qu'il a rédigée en 1996, elle clame à l'adresse des États que « *Le cyberespace ne se situe pas dans vos frontières*.[45] ». Cette approche est guidée par une vision utopiste où la liberté est érigée en valeur cardinale, notamment les libertés d'expression et d'information qui sont protégées par le 1er amendement de la Constitution américaine. La seconde représentation du cyberespace sous-tend les craintes que celui-ci a suscitées notamment chez les autorités étatiques en vertu justement du principe de souveraineté territoriale. En effet, longtemps écartés des évolutions de l'Internet, les États ont souhaité reprendre la main sur ce qu'ils ont perçu en premier lieu comme un moyen pourvoyeur de croissance et un enjeu démocratique, puis dans un second temps un espace qui échappait à leur contrôle et facteur de menaces. Dans cette seconde approche préside une vision dystopique du cyberespace, lequel suscite les craintes de l'avènement d'un panoptique orwellien, nourries du roman *1984* ou plus concrètement des révélations d'Edward Snowden. Ces deux visions se sont étoffées,

[45] https://www.eff.org/cyberspace-independence

imbriquées et brouillées, mais peuvent se résumer à la dialectique actuelle de la liberté et de la sécurité.

### b) *Une vision libérale et libertaire*

La logique de liberté a d'abord prévalu. Le vocable « cyberespace » est un mot-valise formé par la combinaison des termes *cybernétique* et *espace*. Il est apparu pour la première fois sous la plume d'un auteur de science-fiction inspiré par la cybernétique[46]. La paternité de du mot *cybernétique* est communément attribuée à un professeur de mathématiques du MIT de Boston, Norbert Wiener, mais le terme est déjà employé par les Grecs anciens et désigne au XIX$^{e}$ siècle la science du gouvernement des hommes (André-Marie Ampère, 1834). En 1948, ce dernier publie la somme des travaux sur sa « théorie de la commande et de la communication, dans l'animal et la machine »[47]. Le contexte de l'époque est celui de l'essor de l'informatique avec l'apparition des premiers ordinateurs tel l'ENIAC (*Electronic Numerical Integrator And Computer*) en 1945, qui prend la suite des cartes perforées du XIX$^{e}$ siècle et des « bombes » électromécaniques inventées par le célèbre cryptologue britannique Alan Turing pendant la Deuxième Guerre mondiale. Par ailleurs, les conférences de Macy qui se tiennent de 1942 à 1956 et regroupent des spécialistes tant des sciences dures (mathématiciens, physiciens, neurologues) que des sciences humaines (anthropologues, psychologues, économistes…), cherchent à faire émerger une science du fonctionnement de l'esprit. On essaie alors de s'inspirer, par biomimétisme, de la nature du cerveau humain pour créer des équivalents artificiels. Cette suite de débats et d'échanges est à l'origine des sciences cognitives actuelles et de la cybernétique, laquelle va accoucher des sciences de l'information qui seront enrichies par la suite des apports en théorie de la communication de l'école de Palo Alto.

Avec sa théorie cybernétique, Norbert Wiener propose de rationaliser les processus de transmission de l'information à travers la communication, les mécanismes autogérés et le contrôle aussi bien chez les machines que chez l'homme. Le terme est d'ailleurs issu du grec *kubernetes*, qui signifie « timonier » et a donné un champ lexical autour des mots *gouvernail*, *gouverneur* ou encore *gouvernement*. S'en dégage donc une notion de contrôle et de pilotage technique ainsi qu'une dimension politique. Au-delà de l'étude mathématique point aussi, en effet, l'idée d'un discours politique fondé sur les valeurs démocratiques de la transparence et de la communication et légitimé par une caution scientifique[48]. Dans le sillage de la cybernétique, l'émergence de l'Internet et des technologies de la communication va donc

[46] William Gibson, *Neuromancien*, La Découverte, 1985.
[47] Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, Hermann & Cie & MIT Press, 1948.
[48] Alix Desforges, « Les représentations du cyberespace : un outil géopolitique », *in* "Cyberespace : enjeux géopolitique", *Hérodote*, 2014/1-2 (n° 152-153), pp. 67-81.

prendre tout son sens et favoriser une vision libérale du cyberespace à travers l'avènement de la *société de l'information*, ce qu'Herbert Marshall McLuhan préfigure dans les années 1960 comme le *village global* alors que le *réseau des réseaux* n'est pas encore né.

Précisément, dès 1969 le proto-internet est déjà pensé pour la communication. L'ARPAnet en l'espèce, lancé en 1966 par la DARPA[49] et opérationnel trois ans plus tard, est vu comme un outil facteur de progrès considérables. Dans un article intitulé « *L'ordinateur comme dispositif de communication* » et publié en 1968, deux de ses fondateurs les plus célèbres, Joseph Licklider et Robert Taylor, prophétisent : « […] *les hommes communiqueront de façon plus efficace avec la machine qu'en face à face.* […] *Ce seront des communautés reposant non pas sur une localisation commune mais sur un intérêt commun.* […] *L'effet de cet élément sera important, tant sur les individus que sur la société. Tout d'abord, les individus en ligne seront plus heureux car les gens avec lesquels ils interagiront le plus fortement auront été choisis selon leurs intérêts et leurs objectifs communs, plutôt qu'en fonction des hasards de la proximité géographique. Ensuite, la communication sera plus effective et productive, et donc plus agréable*.[50] » Le projet fera en outre l'objet d'une vision fantasmée selon laquelle le réseau en devenir peut résister à une attaque nucléaire et qu'il a d'ailleurs été conçu dans cette optique. En réalité, l'ancêtre de l'Internet a été pensé par des universitaires qui souhaitaient disposer d'une puissance de calcul supérieure car mutualisée et pouvoir échanger des informations avec leurs pairs à travers le réseau des universités du pays. D'ailleurs, les premiers virus informatiques ont été conçus pour partager de l'information entre machines non interconnectées.

Cette vision idéalisée va se prolonger dans la sphère militante et la mouvance libertaire. La contre-culture californienne en particulier milite pour des idéaux communautaires qui imprègnent les valeurs émancipatrices des premiers hackers. Les notions caractéristiques des prérogatives régaliennes, comme celles de territoire, de pouvoir et de hiérarchies verticales sont remises en cause dès les années 1960-1970. Aux promesses de réseaux d'informations décloisonnées répondent les revendications de liberté et de partage des militants. Les informaticiens et surtout les hackers promeuvent la communauté du logiciel libre et/ou *open source*[51], transparent et ouvert. Plus récemment, même si le mouvement social du libre est

[49] Defense Advanced Research Projects Agency, agence de projets de recherche avancés de défense.

[50] Joseph C. R. Licklider et Robert Taylor, « The computer as a communication device », *Science and Technology*, avril 1968, cité par Patrice Flichy, *L'imaginaire d'Internet*, La Découverte, 2001, 276 p., pp. 51-52.

[51] Le logiciel libre, parfois qualifié de « logiciel libérateur », permet juridiquement et techniquement à tout utilisateur de prendre à son compte un programme informatique pour l'utiliser, le modifier, le décliner à sa guise. Il s'oppose au logiciel dit « privateur/propriétaire » vu par les tenants du libre comme un pouvoir indu de contrôle des éditeurs logiciels sur les utilisateurs. Les logiciels *open source* désignent des programmes dont le code source informatique est ouvert, à savoir consultable intégralement par tout utilisateur en vue de sa réutilisation. Bien que différentes, les deux notions vont souvent de pair en favorisant l'esprit de partage et de justice d'accès au

toujours représenté, cet activisme s'est un peu étiolé même s'il forme une communauté vivante et garante des libertés fondamentales dans le monde numérique. Selon le journaliste-hacker Olivier Laurelli, la communauté des hackers s'est divisée notamment en France et une partie est restée ou revenue vers le mouvement par peur des mesures de contrôle étatique visant cet univers marginal[52]. Ceux qui sont restés prônent la libération des connaissances et louent les mérites d'un accès total au savoir scientifique. Ce fut le cas de l'hacktiviste Aaron Swartz, inventeur des licences *Creative Commons*, du site pour les lanceurs d'alerte et journalistes *Securedrop* ou du format de flux de syndication RSS, qui fait le bonheur des veilleurs mais également des usagers des réseaux socionumériques. Poursuivi et possiblement harcelé par la Justice américaine pour avoir piraté et diffusé la base de données universitaire de l'éditeur JSTOR, il connaît un destin tragique en mettant fin à ses jours. Son action sera poursuivie indirectement par une étudiante kazakhe devenue neuroscientifique, Alexandra Elbakyan, qui a fondé le malaimé Sci-Hub, inspiré des propos de McKenzie Wark selon lesquels « *la propriété intellectuelle impose une relation de pénurie. Elle assigne un droit de propriété à un propriétaire, aux dépens de non-propriétaires, à une classe de possesseurs aux dépens de spoliés.*[53] »

Cet activisme s'est prolongé et durci au début de la décennie 1990 dans ce qu'on appelle les *cryptowars* ou « guerres pour la cryptographie », lesquelles ont toujours été considérées comme un garde-fou éthique pour prévenir les ingérences dans la vie privée des internautes. Le phénomène est aujourd'hui très paradoxal car ce procédé très commun sur le Web grand public[54] est à la fois démocratisé et poussé comme un gage de confiance entre d'un côté les fournisseurs de contenus et de produits tel le e-commerce, et les internautes de l'autre ; et dans le même temps perçu par les autorités étatiques comme un danger entravant la lutte contre la cybercriminalité ou le terrorisme. Ces guerres pour la cryptographie ont vu l'émergence d'hacktivistes célèbres comme Julian « Proff » Assange, fondateur de Wikileaks mais d'abord militant du groupe des *Cypherpunks*. Tiré d'un jeu de mot entre cyber et *cypher*, lui-même mot-tiroir signifiant chiffre/chiffrer (*cipher*) et à rapprocher du courant *cyberpunk*[55]. Plaidant pour une gouvernance mondiale anarcho-libertarienne, le groupe a créé des outils de chiffrement, des monnaies et réseaux internet décentralisés[56]. Parmi les héritiers du groupe, la

savoir-faire de programmation. Le logiciel et notamment le cryptosystème de *Whatsapp* est par exemple issu de la messagerie instantanée *Signal*, libre et open source.

[52] Entretien avec l'auteur, 30/03/2023.

[53] https://creativecommons.org/ ; https://securedrop.org/ ; https://sci-hub.se/ ; McKenzie Wark, *A Hacker Manifesto*, Criticalsecret, 2004.

[54] À travers notamment le protocole de chiffrement des communications des sites web, le protocole réseau TLS (*transport layer security*) plus connu sous l'acronyme *https*, *i.e.* le système hypertexte *sécurisé*.

[55] L'ancêtre de Wikileaks est d'ailleurs toujours actif depuis 1996 sur le site https://cryptome.org/. Le *cyberpunk* est un courant littéraire, sous-genre de la science-fiction.

[56] Voir Rayna Stamboliyska, *La face cachée d'internet*, Larousse, 2017, 352 p., pp. 231-238.

mouvance des *Anonymous* parés du masque de Guy Fawkes, héros de la B.D. et du film *V pour Vendetta*, s'est inspirée largement de l'approche moraliste et libertaire des *Cypherpunks*, tout en prenant *in fine* ses distances avec Wikileaks.

La première *cryptowar* s'inscrit dans le contexte de la lutte des autorités américaines contre les logiciels de chiffrement dont elles veulent (CIA et NSA en tête) conserver le monopole en interdisant notamment leur diffusion hors du territoire national. Pendant trois ans, celles-ci vont poursuivre en justice Philip Zimmermann, le créateur du cryptosystème PGP, pourtant aujourd'hui totalement démocratisé dans le chiffrement asymétrique[57]. Connu pour sa formule : « *Si la protection de la vie privée est hors-la-loi, alors seul les hors-la-loi ont droit à une vie privée* », il sera relaxé, selon lui parce que les banques ont vu tout l'intérêt de la cryptographie pour les affaires et pressé l'État d'abandonner les poursuites à son encontre. En France, il faudra attendre la LCEN de 2004 pour que l'utilisation du chiffrement soit autorisée[58]. La deuxième *cryptowar*, quant à elle, a concerné la question du chiffrement en lien avec la lutte antiterroriste à partir de 2015 et n'a *a priori* pas trouvé d'issue. Le débat porte en effet sur la possibilité et la volonté de certains États d'implémenter des « portes dérobées », en anglais *backdoors*[59] dans les logiciels et notamment les messageries instantanées chiffrées plébiscitées depuis quelques années par le grand public. Le Royaume-Uni notamment, avec David Cameron ou Theresa May, ou les États-Unis périodiquement et parfois la France via la voix isolée de quelques élus requièrent en effet cette entorse à la vie privée afin de permettre aux forces de sécurité d'outrepasser les règles de chiffrement et ainsi faciliter l'identification des terroristes. Outre que de telles mesures remettent en cause des droits fondamentaux démocratiques, se pose également la question de leur efficacité. Rayna Stamboliyska, spécialiste et conseillère sur ces sujets auprès d'organisations internationales, indique que la plupart des terroristes prennent leurs précautions et utilisent des moyens traditionnels de communication. Il faudrait selon elle encadrer les actions de lutte contre ce qu'elle estime être des infractions pénales, de terrorisme ou de criminalité selon des principes de nécessité et de

[57] PGP pour *Pretty good privacy* est un logiciel cryptographique fondé sur l'algorithme de chiffrement asymétrique RSA, du nom de ses trois inventeurs (Rivest-Shamir-Adleman). Il permet par exemple de chiffrer les pages web (https), qui utilisent ce type de chiffrement asymétrique en combinaison avec un chiffrement symétrique. Le chiffrement asymétrique nécessite la génération d'une paire de clés cryptographiques appelée souvent « trousseau » (clé publique, non sensible ; clé privée, secrète) alors que le symétrique utilise une seule et même clé secrète. Le RSA a permis de dépasser le problème de confidentialité que posait le partage de clés symétriques.

[58] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164, cité par Rayna Stamboliyska, *op. cit.*, p. 299.

[59] Une *backdoor* ou « porte dérobée » désigne, en informatique, un accès secret aux données d'un utilisateur à travers un équipement matériel (puces électroniques…) ou un logiciel (dans son code) permis à un acteur tiers, à l'insu de l'utilisateur desdites ressources. S'il est assez facile de détecter une backdoor logicielle, les portes dérobées matérielles sont, quant à elles, extrêmement difficiles à détecter car la conception des processeurs est protégée par la propriété intellectuelle (Voir le documentaire *Cybercriminalité, des attaques bien réelles*, Arte, Allemagne, 2023, 1h39, à 28:40mn). Les composants ou logiciels forment alors de véritables *chevaux de Troie* (*trojans*).

proportionnalité[60]. Par ailleurs, nombre de membres des forces de l'ordre plaident contre ce type de pratiques en arguant que cela détériorerait la confiance sur laquelle une très large part de l'espace numérique est fondée avec la cryptographie, que c'est une difficulté avec laquelle il faut composer et qu'il existe d'autres moyens pour appréhender les criminels sans avoir à décrypter leurs données[61].

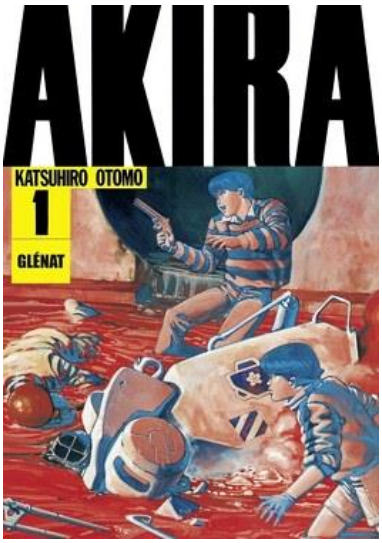
Tout cet imaginaire fondé sur la liberté et la résistance à l'obscurantisme va également baigner le monde politique qui, dans les années 1990, embrasse la révolution numérique qu'induit l'Internet. Tour à tour qualifié de « facteur d'égalité » ou « d'enjeu démocratique », l'Internet et plus tard les réseaux socionumériques (RSN) vont nourrir un discours libéral axé sur des enjeux de développement économique et social. Aux États-Unis, Al Gore évoque les « autoroutes de l'information » de la *Global Information Infrastructure* (GII) censée encourager la participation politique et servir l'intérêt commun. Tandis qu'en France, on alerte sur une possible « fracture numérique » et on loue l'accès généralisé au savoir et à la culture, et la participation citoyenne. Cette effervescence d'optimisme sert bien entendu les entreprises commerciales qui vont tôt faire leur miel de cette manne numérique. Le cyberespace devient bien plus qu'un réseau informationnel global, il est une entité en soi porteuse de tous les espoirs. Et l'objet, déjà, de toutes les manipulations. Dès le début, William Gibson, inventeur du vocable, sait qu'il a créé un « mot à la mode », un artifice diégétique qui va dépasser le seul cadre narratif de la science-fiction et de la culture *geek* pour devenir un *acte de communication*, comme le diminutif « cyber » ou la « data » aujourd'hui. Il souligne dans un interview en l'an 2000 : « *j'ai su, dès que j'ai eu la première scène, que je tenais quelque chose de complètement nouveau.* [...] *Le "Cyberspace Sept" permet d'accéder au "non-espace incolore de la matrice de simulation, l'hallucination consensuelle électronique qui facilite les manipulations et l'échange d'énormes quantités de données.* [...] *J'en étais arrivé à un point où il me fallait un mot à la mode. J'avais besoin de remplacer le vaisseau spatial et le holodeck par quelque chose qui serait un signe de changement technologique et qui me fournirait un moteur narratif et un territoire où la narration pourrait avoir lieu.* [...] *Tout ce que je savais du mot cyberspace quand je l'ai inventé, c'est qu'il avait l'air d'être un mot à la mode efficace. Il était évocateur, mais essentiellement dénué de sens.* [...] *Il suggérait quelque chose, mais n'avait pas de vrai sens sémantique, même pour moi, quand je l'ai vu émerger sur la page.*[62] »

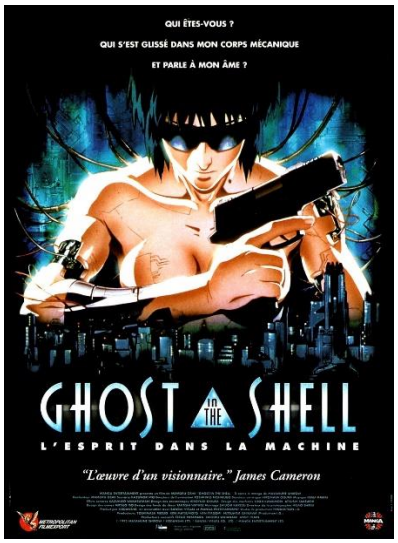
[60] Rayna Stamboliyska, *op. cit.*, p. 299.
[61] Entretien avec Fabrice Crasnier, 13/10/2017. Fabrice Crasnier est expert en informatique et ancien officier de gendarmerie.
[62] *No Maps For These Territories*, film documentaire de Mark Neale, REEL23, 2000, cité par Audrey Lohard, « La genèse inattendue du cyberespace de William Gibson », *in* "Cyberesp@ce & territoires", *Quaderni*, n°66, 2008, pp. 11-13.

Toutefois, après avoir suscité les plus grands espoirs, le cyberespace va faire naître la crainte, parfois tout aussi extrême, de menaces critiques pour les sociétés humaines et surtout les États.

### c) *Une vision anxiogène et sécuritaire*

Trente-six ans après la cybernétique de Norbert Wiener, le néologisme « cyberspace », en anglais comme dans sa traduction française dans le texte, apparaît dans une œuvre de fiction qui fonde le genre littéraire *cyberpunk*. C'est dans le roman de science-fiction *Neuromancien*[63], publié en 1984, que William Gibson utilise donc pour la première fois le concept en des termes nébuleux qui, s'ils dépeignent un univers dystopique typique du genre, font parfois écho aux réalités de notre époque technologiste. Le roman met en scène un hacker voleur de données qui connecte son esprit à un réseau mondial d'ordinateurs. Dans les années 1980, le genre cyberpunk va générer tout un imaginaire qui va essaimer dans les 7e, 9e et le parfois consacré 10e art, le jeu vidéo. Il a ses propres œuvres cultes, notamment dans la B.D. avec *Akira* (Katsuhiro Ōtomo) ou *Ghost in the Shell* (Masamune Shirow) ou dans le cinéma des soeurs Wachowski et leur tétralogie *Matrix* post-cyberpunk, ou surtout le fameux *Blade Runner* de Ridley Scott adapté du roman de Philip K. Dick, *Les androïdes rêvent-ils de moutons électriques ?*[64] Le cyberpunk est une projection dystopique dans un univers sombre, cynique et décadent où la technologie a pris le dessus sur l'humain, au point que celui-ci s'hybride progressivement aux machines dans une logique transhumaniste.





[63] William Gibson, *Neuromancien*, La Découverte, 1985. Le terme apparaît pour la toute première fois dans sa nouvelle *Burning Chrome*, publiée en 1982.

[64] Katsuhiro Ōtomo, *Akira*, Kōdansha, Japon, 14 vol. ; Masamune Shirow, *Ghost in the Shell*, 1989-1991, Kōdansha, Japon, 2 vol. ; Ridley Scott, *Blade Runner*, film cinématographique, États-Unis, Warner Bros, 1982, 111/117mn ; Philip K. Dick, *Do Androids Dream of Electric Sheep?*, Doubleday, 1968, 229 p.

Si cette représentation paraît outrancière, elle demeure ancrée dans l'inconscient collectif du fait de l'essor fulgurant des progrès des technologies de l'information-communication en ce début de XXIe siècle. Face à cet espace diffus, décentralisé et impalpable, les États éprouvent les plus grandes difficultés à exercer leur pouvoir et leur autorité. Le cyberespace semble en effet rétif à toute idée d'appropriation et de contrôle. En avril 2007, après une série d'attaques par déni de service paralysant une large partie de ses institutions, l'Estonie par la voix de son ministre de la Défense annonce « la Troisième Guerre mondiale »[65]. Redoutant la criminalité appliquée à ce nouvel environnement, souvent débordées par des mouvements socio-communicationnels puissants issus du Web, les autorités gouvernementales ont toutes construit des discours *sécuritisés* vis-à-vis de la cybermenace[66]. Dans un réflexe traditionnel, elles ont appréhendé le cyberespace comme un territoire à sécuriser jusqu'à en faire un nouveau champ de bataille sur lequel une cyberdéfense se déploierait. Cette territorialisation a engendré un besoin de légifération et de maîtrise géopolitique, passant par la volonté de contrôler les infrastructures matérielles de l'Internet mais aussi les informations qui y transitent. L'affaire Snowden a bien évidemment permis de prendre la mesure de cet effort de maitrise sur les véhicules de l'information et de surveillance sur les données elles-mêmes. Parmi les programmes de la *National Security Agency* (NSA*), *PRISM* est le plus remarquable puisqu'il contraignait – et contraint toujours indirectement – les *Géants du numérique* américain à contribuer à cette collecte généralisée d'informations privées, sous couvert de la loi du *Patriot Act* puis du *Cloud Act* depuis 2018[67]. Par analogie, ces dispositions forment de vraies « backdoors juridiques ».

Ainsi, quand les hacktivistes justifient leurs actions et par exemple des attaques informatiques au nom de la sauvegarde des libertés collectives et individuelles, les États légitiment la lutte contre la cybermenace et leur contrôle de l'espace numérique par la protection des citoyens et des institutions. Or, cette cybermenace est difficile à appréhender. C'est d'ailleurs pour cette raison que beaucoup d'États notamment européens ont tardé à comprendre qu'objet, enjeu et avers du modèle démocratique, l'information pouvait aussi bien en constituer le revers. En France, l'ANSSI identifie aujourd'hui quatre principales menaces

[65] Imputées à la Russie, ces cyberattaques interviennent par suite du déplacement de la statue du soldat de bronze soviétique du centre de Tallinn vers sa banlieue.

[66] La *sécuritisation* (et non sécurisation) est un concept constructiviste issu de la théorie des Relations internationales. Il rend compte de la politisation extrême – plus ou moins délibérée – de l'enjeu sécuritaire. En d'autres termes, un phénomène social, politique, etc. est érigé et traité (acte de langage) en enjeu de sécurité.

[67] Le *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) est une loi américaine promulguée en mars 2018 pour contrer la législation européenne à venir de mai 2018 du RGPD (Règlement général de protection des données). Elle permet aux autorités judiciaires d'accéder aux données des entreprises de droit américain stockées à l'étranger. Parmi celles-ci on compte notamment des services de *cloud computing* (comme AWS, le Cloud d'Amazon qui représente une part de marché de 34% dans ce secteur. Avec Google Cloud et Microsoft Azure, ce nombre se porte à plus de 60% - https://fr.statista.com/infographie/17825/parts-de-marche-cloud-infrastructure-par-fournisseur/)

liées au cyberespace : la déstabilisation, l'espionnage, le sabotage, la cybercriminalité[68]. Mais cette menace est protéiforme et difficile à inventorier. Ses acteurs sont disparates et leurs actions peuvent aller de l'escroquerie en ligne par un cyberdélinquant à des malwares très élaborés provenant de la recherche informatique au sein d'entités étatiques, disposant par ailleurs d'une masse critique en termes de ressources et d'infrastructures numériques et matérielles, en passant par des atteintes à la réputation du fait de simples individus ou de collectifs restreints. Le risque cyber est ainsi régulièrement classé en deuxième place par les experts.


**Figure 1 :** *Évolution du classement des trois premiers risques selon la banque-assurance Axa*[69]

Par ailleurs, les techniques et outils malveillants utilisés sont polyvalents et peuvent être indifféremment employés à des fins et par des acteurs de diverses natures. Par exemple, des programmes malicieux peuvent servir à la fois des objectifs d'espionnage ou de cybercriminalité car les armes numériques sont modulaires et plastiques : elles peuvent comporter plusieurs briques logicielles pour autant d'usages à la demande : *stealers*, *keyloggers*, interfaces de commande et contrôle (C2), outils d'administration à distance (RAT), *ransomwares-wipers*…[70] De même, des cyberterroristes peuvent procéder à des attaques de

[68] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf (rapport du panorama 2022 de la cybermenace selon l'ANSSI). Pour un panorama synthétique de la cybermenace, l'on pourra opportunément se reporter à Nicolas Arpagian, *La cybersécurité*, *op. cit.*

[69] https://www.axa.com/fr/actualites/future-risks-report-2022

[70] Un *stealer*, littéralement « voleur » est un logiciel espion (*spyware*) collectant des informations spécifiques d'authentification comme des *tokens* de session web ou des identifiants de connexion. Un *keylogger* est un logiciel (ou un dispositif physique proche d'une clé USB) enregistrant les frappes de clavier saisies sur un ordinateur. Relié à un C2 il peut notamment transmettre par l'internet les sessions de frappes collectées à un serveur pirate distant. Un *ransomware* est un logiciel chiffrant les données d'un SI (les rendant indisponibles) et lié à une opération de rançonnage/chantage.

défacement[71] d'un site web légitime, mais un individu par jeu ou activisme peut de la même façon s'introduire dans ledit site via une même faille de sécurité pour réaliser cette atteinte à l'image. Généralement, la faille a trait à un défaut de configuration du système d'exploitation d'un serveur, une mauvaise sécurisation des droits d'accès administrateurs ou encore la compromission d'une base de données (BdD) relationnelle via des *injections SQL*[72]. En outre, cette attaque peut très bien être le fait d'un État ou d'un groupe de hackers-corsaires sous « faux drapeau » (*false flag*). C'est vraisemblablement ce dont a été victime la chaine francophone TV5 Monde, en plus de subir une attaque *par déni de service* : en 2015, ses services et chaines sont mis à l'arrêt par une série d'attaques informatiques. La page d'accueil de son site web est défacée et arbore la mention « cybercaliphate » faisant penser à un acte cyberterroriste dans le contexte d'alors. Il s'avère que plusieurs indices concordants vont orienter les analyses inforensiques dites *post-mortem* vers la piste des hackers-corsaires russes APT28, alias les *Fancy Bears*[73].

La prise en compte, au demeurant sérieuse, de ces menaces diffuses et globales par les États a créé un vrai sentiment d'insécurité globale nourri par les médias mais aussi des entreprises privées qui évoluent dans ce qui est devenu un véritable marché de la cybersécurité[74]. Ce terme fait du reste débat et on lui préfère en France la notion de sécurité des systèmes d'information. Toutefois, à notre sens, la cybersécurité n'a pas usurpé sa place, puisqu'elle envisage la mise en sûreté et en sécurité[75] de l'ensemble des actifs du cyberespace dans une approche holistique. Mais ceci fait débat. Parfois considérée comme un sous-ensemble de la sécurité informatique, il nous semble au contraire que la cybersécurité consiste en une vision d'ensemble des lois, politiques, outils, procédures, méthodes, en un mot des actions visant à protéger les systèmes d'information *lato sensu* (*i.e.* sociotechniques)[76]. Le terme, qui vient de la langue de Shakespeare est d'ailleurs mal traduit dans celle de Molière, puisqu'il devrait être question de « cybersûreté ». En réalité, mesures de sûreté et de sécurité

[71] Opération de « vandalisme informatique » consistant à modifier les ressources d'une page web, généralement l'accueil d'un site pour revendiquer un message généralement politique.

[72] Une SQLi ou « injection SQL » (*Structured Query Language*, un langage de programmation de BdD très usité) consiste à injecter du code qui va détourner les politiques de requêtes normales d'une base de données.

[73] Une attaque par déni de service (D/DOS, *distributed/denial of service*) désigne la saturation d'un site web par la génération massive (généralement distribuée, *i.*e. utilisant un *botnet*, un réseau d'ordinateurs mutualisé) de requêtes de connexions synchrones à la ressource. Les serveurs du site sont saturés et le service devient inopérant.

[74] Alix Desforges, « Les représentations du cyberespace : un outil géopolitique », *op. cit*., pp. 78-79.

[75] La sûreté concerne les mesures mises en place contre des risques de malveillance ; la sécurité, les mesures pour prévenir des risques d'accidents. Exemple en informatique : se prémunir contre le vol de son ordinateur (sûreté) ; anticiper la panne ou la perte de son ordinateur (sécurité).

[76] C'est du reste l'approche de l'Union internationale des télécommunications (UIT, ONU), https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

s'appliquent pareillement à l'environnement numérique, y compris dans l'acception politique de ces termes : sûreté comme approche objective et sécurité comme abord subjectif.

Ainsi, le cyberespace demeure un concept complexe qui fait l'objet de deux principales représentations : espace de libertés a-territorial et territoire plus ou moins matérialisé que les États cherchent à maîtriser. Dans les deux cas, les nombreuses parties prenantes du domaine numérique tentent d'y exercer leur souveraineté par le biais de la force et de la ruse.

### **2)** Un champ d'expression de la force et de la ruse

« *Il n'y a que deux puissances au monde, le sabre et l'esprit : à la longue, le sabre est toujours vaincu par l'esprit*. »

Napoléon Bonaparte

Dans *Les théories du pouvoir* publié en 1994, la philosophe Jacqueline Russ dévoile les arcanes des jeux qui, précisément, ne se trament plus seulement au cœur des palais.

> « *Des normes, des pouvoirs, des systèmes d'information : le pouvoir contemporain dessine ses multiples figures sur fond de société ouverte, à l'intérieur d'un ensemble dynamique. Une société, en effet, ne se définit pas seulement par des règles contraignantes et le maintien d'une organisation. Elle désigne aussi un système ouvert et une capacité adaptative.* […] *Le pouvoir contemporain gère, avec une subtilité extrême, le désordre qu'il prend en charge. Tout pouvoir, nous le savons, gère le désordre. Or cette gestion actuelle du désordre s'opère par des systèmes de communication, par des normes, par des stratégies ouvertes, par des dominations masquées et déguisées.*[77] »

Ce désordre, c'est celui qu'a accentué la mondialisation et ses promesses illimitées de possibles. C'est celui de la mise en réseaux et en interdépendance des sociétés et activités humaines. Le cyberespace est ainsi le « lieu », l'agora ultime et globale où la reprise en main et un ordre anarchique (sans vraie hiérarchie) est rétabli par les plus opportunistes des acteurs, ceux qui en maîtrisent et savent exploiter les rouages et les effets de levier. C'est l'espace qui unit les systèmes d'information et de communication et où se déploient au mieux les stratégies masquées et couvertes de la domination.

Le cyberespace est en effet un domaine où l'exercice machiavélien de la puissance trouve des débouchés féconds. Force et ruse se combinent jusqu'à fusionner dans l'emploi de cet espace qui se caractérise avant tout par son insaisissabilité. C'est la nature même du

[77] Jacqueline Russ, *Les théories du pouvoir*, Le livre de poche, 1994, 349 p., pp. 313-318. Cité par Nicolas Moinet, *Les sentiers de la guerre économique.* T2 – *"Soft Powers"*, VA, 2020, 182 p., pp. 12-13.

cyberespace qui conditionne ses acteurs à utiliser la dissimulation, l'artifice et l'approche indirecte y compris dans le cadre d'attaques dites cyber-physiques encore rares[78]. Il véhicule souvent dans un même mouvement des mesures coercitives et des opérations d'influence. Prenons pour exemple les offensives informationnelles attribuées à la Russie : elles comportent systématiquement des attaques informatiques et des manœuvres de cyber-influence. Mais à l'image du sabre vaincu *in fine* par l'esprit, les attaques physiques sur les infrastructures ou les atteintes plus immatérielles sur les couches logique et humaine du cyber ont une portée en définitive plus psychologique que cinétique. Avec, pour autant, des effets aussi ravageurs.

#### a) *L'usage de la coercition plus que de la force…*

L'usage de la force à travers le cyberespace et en son sein est le fait des forces armées qui ont depuis les années 2000 produit une littérature doctrinale aujourd'hui bien fournie. Appréhendé comme un espace de bataille en soi mais surtout complémentaire des milieux géographiques naturels (terre, mer, air, espace exo-atmosphérique) où s'exerce le feu, le champ numérique autorise des effets démultiplicateurs dans notre monde physique. À l'orée des années 1990, la réflexion sur l'articulation entre la guerre et les technologies de l'information se matérialise aux EUA dans une *Révolution sur les affaires militaires* (RMA*), qui annonce le concept de *numérisation du champ de bataille*. Cet aggiornamento de la pratique guerrière vise la supériorité informationnelle par le biais d'une *guerre réseau-centrique* (NCW*)[79]. Préfigurée par les Soviétiques[80], conceptualisée et mise en pratique par l'armée américaine, la NCW se fonde sur la mise en réseaux des systèmes d'armes, de transmission-communication, commandement et unités militaires. Le partage technique de l'information en temps réel permet ainsi d'améliorer l'intelligence situationnelle, favorise l'émergence d'armes dites « intelligentes », et accélère la décision et son application entre chaine de commandement et courroie opérationnelle. La France parle aujourd'hui d'*infovalorisation*[81]. Mais cette approche reste largement technicienne et constitue une fonction de soutien au combat. Dès lors, la force emprunte une voie plus proche de la contrainte en dissuadant d'agir, et forme par là même un des marqueurs de la cyberpuissance.

Si l'on parle bien et à raison d'*armes numériques*, leur usage permet paradoxalement d'atténuer le degré de violence d'une action offensive. Celles-ci n'engendrent précisément aucun effet létal du moins direct ; comme *a fortiori* les attaques purement informationnelles

[78] Les attaques cyber-physiques consistent à impacter des éléments matériels dans l'environnement physique par le biais d'attaques informatiques. Elles visent généralement les systèmes de sécurité industriels et toucheront vraisemblablement de plus en plus les objets connectés. Voir le cas Triton dans la partie 2.
[79] *Network Centric Warfare*. Le concept sera développé en partie 2.
[80] Bertrand Boyer, *Cybertactique*. *Conduire la guerre numérique*, Nuvis, 2014, 243 p., p. 107.
[81] Voir par exemple https://hal.science/hal-01823344/document

de nature sémantique. On pourrait donc avancer que ce type d'armes nouveau constitue une modalité de la force car portant atteinte à des dispositifs de protection logique[82] ou plus simplement des systèmes d'information à caractère privé. Or, cette aptitude d'acteurs publics souvent couplés à des acteurs privés matérialise ce que Jean-Louis Gergorin et Bernard Barbier appellent la *cyber-coercition*[83]. Le cyberespace autorise les opérations informatiques et informationnelles à moindre coût par des États cherchant à défendre leurs intérêts en usant – plus qu'en menaçant d'user – de mesures indirectes et « *peu chères, en créant ou amplifiant des forces ou des évènements de nature à affaiblir la cible et d'améliorer leur rapport de force avec elle. L'opération cyber, au contraire d'un acte d'agression matériel, risque peu d'engager dans une escalade conduisant à la guerre* [...]. *Ces techniques, compte tenu de leurs caractéristiques de discrétion, leur faible coût, leur progressivité et le caractère fréquemment réversible de leurs effets, peuvent même être utilisées contre des pays amis, c'est-à-dire par tout le monde et contre tout le monde.* [...] *L'un des résultats de ce développement du cyber sera, je crois, la mise en place de stratégies de "cyber-coercition" : réagir à des actions jugées hostiles d'un adversaire en lui montrant qu'on peut lui faire beaucoup de mal. C'est ce qu'a fait la Russie avec l'Estonie.* [84] »

Au-delà de cette mise en garde et reprenant les propos du directeur de l'ANSSI d'alors, Guillaume Poupard, certains États prépositionneraient des « implants logiciels » au sein d'infrastructures critiques pouvant faire l'objet d'une exploitation ultérieure en vue de neutraliser ces dernières[85]. La cyber-coercition constitue donc une forme de dissuasion d'agir politiquement et peut ainsi se ranger dans la modalité du *sharp power* via le *cyber power*. Il s'agit donc de pratiques qui paraissent convoquer la force, la menace de son usage ou à tout le moins un type de contrainte. Mais plus encore qu'en tout autre lieu, le *topos* numérique allie dans une subtilité aigue la force et la ruse. À cet égard, la mention « d'implants logiciels » est parlante, qui peut être assimilée en quelque sorte à une cinquième colonne malicielle infiltrée chez le rival. Ainsi, la coercition suppose finalement tout autant la ruse quand on s'intéresse aux logiciels. Or, les attaques numériques peuvent avoir lieu sur les trois strates du

[82] Par exemple, on y reviendra, les attaques de *cracking* dites significativement de « force brute » consistent à forcer – logiquement – l'équivalent d'une porte – numérique – fermée à clé.
[83] https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html, consulté le 12/04/2023.
[84] Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?*, Institut Diderot, juillet 2022, pp. 6, 24. (https://www.institutdiderot.fr/les-publications-de-linstitut-diderot/cyber-quelles-strategies-face-a-lexplosion-des-menaces/, consulté le 13/04/2023).
[85] Voir l'article du *Monde* précité, et la proposition de loi de l'Assemblée nationale déposée en 2020 pour y pourvoir (https://www.senat.fr/rap/r20-678/r20-678_mono.html). Jean-Louis Gergorin parle de possible « *paralysie mutuelle assurée entre Russes et Américains* » à propos d'implants prépositionnés dans les réseaux électriques (Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber…*, *op. cit.*, p. 39.)

cyberespace. Présentons-les et détaillons-en les caractéristiques essentielles afin d'apprécier toute la richesse de combinaisons possibles qui permettent de déstabiliser son adversaire.

### b) *Les trois couches d'un espace d'expression de la force et de la ruse*

Comme le souligne métaphoriquement Jean-Vincent Holeindre, la guerre est toujours l'association d'Ulysse et d'Achille, et la ruse du renard n'est ainsi jamais dissociée de la force du lion[86]. C'est bien l'art de la guerre hybride qui règne dans le cyberespace.

- *La première couche est la couche physique. Elle est synonyme de forts enjeux de souveraineté.*

C'est la colonne vertébrale du cyberespace, sorte de moëlle épinière innervant par ses flux de données binaires l'ensemble du corps numérique. Elle est faite de « tuyaux » et de « nexus ». C'est la partie visible et matérielle du cyberespace, qui sépare le monde physique du monde immatériel. Elle est formée des réseaux d'équipements informatiques (routeurs…), des câbles sous-marins et terrestres de fibre optique, de liaisons ou télécommunications (dont les systèmes satellitaires, les ondes radio, les réseaux de téléphonie…) interconnectant des terminaux (ordinateurs, smartphones, objets connectés…) et des serveurs informatiques. Chacune de ces machines forment donc des nœuds par lesquels transitent les flux de données et d'informations.

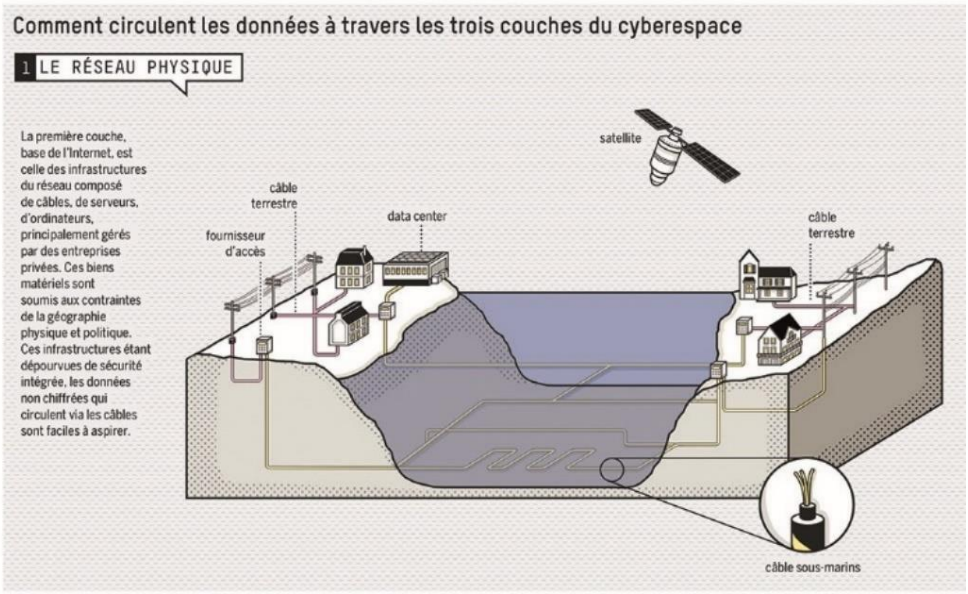



**Figure 2 :** *Schéma simplifié de la première couche (physique)*

Source : « Le Cyberespace. un enjeu de géopolitique majeur », F. Douzet, *Le Monde*, 22-23/07/18.

[86] Jean-Vincent Holeindre (dir.), « Les deux visages de la guerre », in *La ruse et la force. Une autre histoire de la stratégie*, Perrin, 2017, 467 p., pp. 387-390.

Toutes ces ressources sont duales, gérées par des entreprises privées ou parapubliques, employées par les civils comme les militaires. Cette couche est soumise à des attaques logiques et physiques, voire électromagnétiques. Il est difficile de cartographier les interactions entre tous ces systèmes (état de connectivité générale d'un État, répartition et composition des équipements de gestion des réseaux…)[87]. Par ailleurs, la localisation précise des stations d'atterrage, faisant l'interface terre–mer/câbles de fibre optique maritimes–terrestres, sans être tenue secrète (on peut les identifier partiellement sur *Google Maps* par exemple), fait l'objet d'une certaine discrétion puisqu'elles sont critiques, à l'image des composantes du système réticulaire de cette couche. Certaines infrastructures peuvent ainsi comporter un caractère vital, et être ciblées. Ici, le vecteur d'attaque relève bien de la force pure, car le plus souvent on peut bombarder des stations, saboter en les rompant les câbles (notamment dans les eaux internationales), sans compter « *les actions de renseignement, de censure et de vol de composants*.[88] »

Plus proche de la ruse, sont envisagées des cyberattaques logicielles type hacking des contrôles de systèmes de gestion de réseaux au sein des stations d'atterrage. Celles-ci pourraient occasionner une altération importante des flux de données voire un arrêt du trafic[89]. De surcroît, on sait grâce aux papiers Snowden que la NSA et son homologue britannique, le *Government Communications Headquarters* (GCHQ*), ont opéré – comme d'autre États aujourd'hui – des captations de données via du renseignement d'origine électromagnétique (ROEM/SIGINT*)[90]. Bien évidemment, on se situe pour ces cas d'emploi au niveau d'opérations militaires. Mais ces infrastructures sont de nature et de conception civiles. D'où une imbrication complexe en termes juridiques, notamment sur le plan du droit des conflits armés. Comme souvent en droit, tout est relatif à l'intention. D'un point de vue économique, en outre, se pose la question de la fabrication des équipements et câbles, de leur pose et maintenance. Quatre acteurs se partagent le premier secteur : l'Américain TE SubCom (AT&T), le Japonais Nec Submarine System, le Chinois Huawei Marine Networks (HMN Technologies) et le Français Alcatel Submarine Networks (ASN), étant entendu que cette entreprise à forte participation nationale appartient dans les faits au groupe finlandais Nokia depuis son rachat d'Alcatel-Lucent en 2015. Quant aux poseurs de câbles (navires-câbliers), on retrouve ASN et Orange Marine, TE Subcom, Optic Marine notamment. Surtout, compte tenu de leurs ambitions et besoins en capacité de transmission de données, les GAFAM (hormis Apple) investissent massivement dans la propriété et les projets de construction et déploiement de

[87] Bernard Boyer, *Cybertactique*, *op. cit.*, p. 95.
[88] Camille Morel, *Les câbles sous-marins*, Biblis, 2023, 200 p., p. 42. Cet ouvrage est issu d'une thèse de doctorat en droit public (*L'État et le réseau mondial de câbles sous-marins de communication*, 2020, université de Lyon 3).
[89] Tara Davenport, « Cyber Attacks Against Submarine Cables: Gaps in International Law », *Submarine Networks World*, Center for International Law, National University of Singapore, 2018, cité *in* Camille Morel, *ibid.*, p. 42.
[90] Ce projet a été baptisé *Upstream*.

câbles à hauteur de 50% des fonds placés dans ces secteurs. Certains, comme Meta, Microsoft ou Google envisagent même de maîtriser l'ensemble de la chaine jusqu'à devenir de probables fournisseurs d'accès à internet (FAI/ISP*).

Au bilan, la couche physique du cyberespace porte de forts enjeux de souveraineté en s'inscrivant en très large part dans l'environnement physique et peut donc être soumise aux règles du territoire, sans pour autant éviter un flou juridique lié aux questions hauturières. On se situe entre la force et la ruse, bien qu'elle fasse la part belle à la première si l'on considère au pire la destruction de ses éléments, au mieux leur neutralisation (logicielle). Toutefois, elle pose deux questions fondamentales qui se placent indubitablement dans la catégorie de la ruse : en premier lieu, celle des composants matériels qu'on utilise. Ces derniers sont-ils souverains ? Sont-ils étrangers ? Avec le risque inhérent que cela comporte concernant les menaces de contrôle via *backdoors*, tant matérielles que logicielles. Citons le programme *Bullrun* révélé par Edward Snowden qui associait NSA, GCHQ et entreprises privées dont la finalité inavouable consistait à introduire des vulnérabilités *by design* dans des systèmes de chiffrement commerciaux : protocoles web, certificats SSL/TLS (https), VPNs, VoIP, vol de clés cryptographiques d'autorités de certification[91]. Prenons aussi pour exemple la Lituanie, qui affirme avoir détecté des *spywares* et des applications natives qui censureraient certains messages (SMS) sur des smartphones de fabrication chinoise. Or, on sait que l'Union européenne n'a décidé que très récemment (juillet 2023) la création d'une filière de semi-conducteurs souverains[92]. En second lieu, où se situent physiquement la plupart des serveurs et data centers, et par où transitent les données des tuyaux acheminant les contenus du Web, principale application de l'Internet, lui-même composante prédominante du cyberespace ? L'enjeu de la *datalocalisation* est ainsi prégnant dès lors qu'en pratique 80% du trafic de données numériques de stock et de flux siègent et passent par le territoire américain. Ce qui démontre factuellement la dépendance techn(olog)ique d'une vaste majorité des pays mais aussi de la France aux EUA[93]. Entre cette donnée physique mais aussi logique du fait de l'oligopole des GAFAM, fournisseurs de services/contenus, « *70% à 80% des données des utilisateurs français transitent par les États-Unis*. […] *la consommation des citoyens français de produits et de services numériques* [est] *captée par de grandes plateformes*

[91] https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html. De même, l'affaire Crypto AG est édifiante. Cette entreprise suisse, fournisseur de solutions de chiffrement, fut contrainte puis rachetée en sous-main par la CIA et le Service fédéral de renseignement allemand pour introduire des portes dérobées dans ses produits pendant un demi-siècle, de 1960 à 2010 auprès de clients issus de 120 pays (voir notamment https://www.marianne.net/monde/crypto-ag-l-entreprise-suisse-qui-permis-la-cia-d-espionner-120-pays-pendant-quarante-ans)

[92] https://www.vie-publique.fr/en-bref/290575-ue-developper-lindustrie-des-semi-conducteurs-en-europe

[93] Seuls de rares États inversent le ratio données souveraines/données dépendantes : la Russie et la Chine notamment, dont le trafic se situe à 80% sur leur territoire, et 20% en dehors. C'est l'exact inverse avec les pays européens en particulier.

*américaines*.[94] » Ces *géants du Net*, comme on les désigne schématiquement, jouent un grand rôle dans le fonctionnement et certains services incontournables du Web mais ils ne contrôlent pas l'Internet, pas plus que quiconque[95]. On l'a vu, ils participent à l'édification de la première couche du cyberespace – mais ils sont surtout prédominants sur les deux autres.

Cette première strate s'articule intrinsèquement à la deuxième pour former ce que l'on appelle les couches basses du cyberespace. Dans la théorie des réseaux informatiques, on utilise généralement un modèle de sept couches appelé *Open Systems Interconnection* (OSI), qui permet de rationnaliser et appréhender la complexité de cette charnière *physico-logique*. Bien qu'il ait été supplanté rapidement par le modèle TCP/IP de quatre couches, l'OSI reste toutefois encore valable théoriquement, plus fin et utile pour saisir le fonctionnement de la communication entre machines.

### c) … *avec une prime pour la ruse*

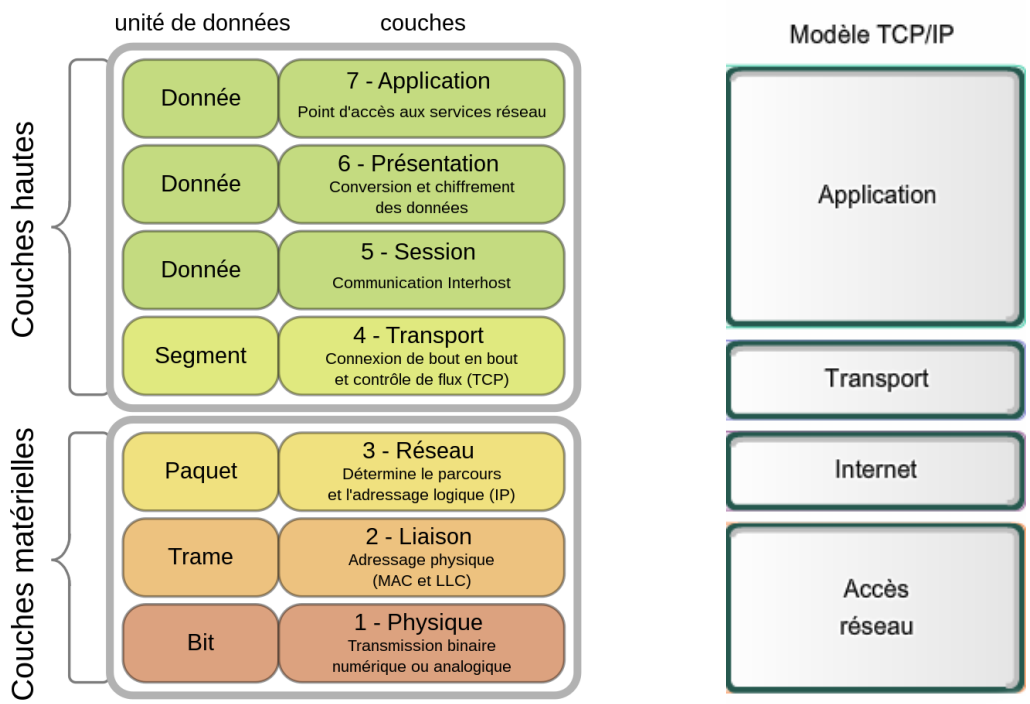



**Figure 3 :** *Modèle OSI, guide pour l'interopérabilité et la communication entre ordinateurs ; modèle simplifié TCP/IP*

Source : https://fr.wikipedia.org/wiki/Modèle_OSI ; https://fr.wikipedia.org/wiki/Couche_réseau

[94] Camille Morel, *op. cit*., p. 94.

[95] Stéphane Bortzmeyer, *Cyberstructure : L'Internet, un espace politique*, C&F Editions, 2018, 270 p., p. 85. La « gouvernance de l'internet » est complexe et mobilise des acteurs publics et privés. S. Bortzmeyer le définit comme un bien commun géré sans hiérarchie mais sans égalité pour autant entre : les États, éditeurs de logiciels, opérateurs réseaux, hébergeurs de serveurs, fournisseurs de services et contenus (souvent dans un rapport de force avec les FAI et les États), organismes de normalisation technique (IETF, W3C) et de régulation (ICANN…).

Ces différents modèles relèvent de normes techniques-informatiques. Du point de vue des sciences humaines et sociales, il est retenu conventionnellement une approche en trois couches, dont la troisième n'apparait pas réellement sur ces modèles, car elle est spécifiquement liée à l'humain. Mais voici pour l'heure détaillée la deuxième strate.

- *La deuxième couche est la couche logique. Loi du code et hackers y règnent en maîtres.*

Cette couche est aussi qualifiée de « syntaxique » car elle agence la couche la plus basse du langage machine et la couche haute dite parfois « humaine ». C'est par cette strate que le cyberespace se construit et se règlemente le plus, via des normes, du code et des protocoles de communication qui permettent aux logiciels d'être interopérables et par extension différents ordinateurs également. Ces logiciels permettent d'automatiser des tâches/processus de calcul par instructions. Cette couche est ainsi vulnérable aux injections de code dans les programmes informatiques ou modifications d'instructions logicielles ou altérations de données.

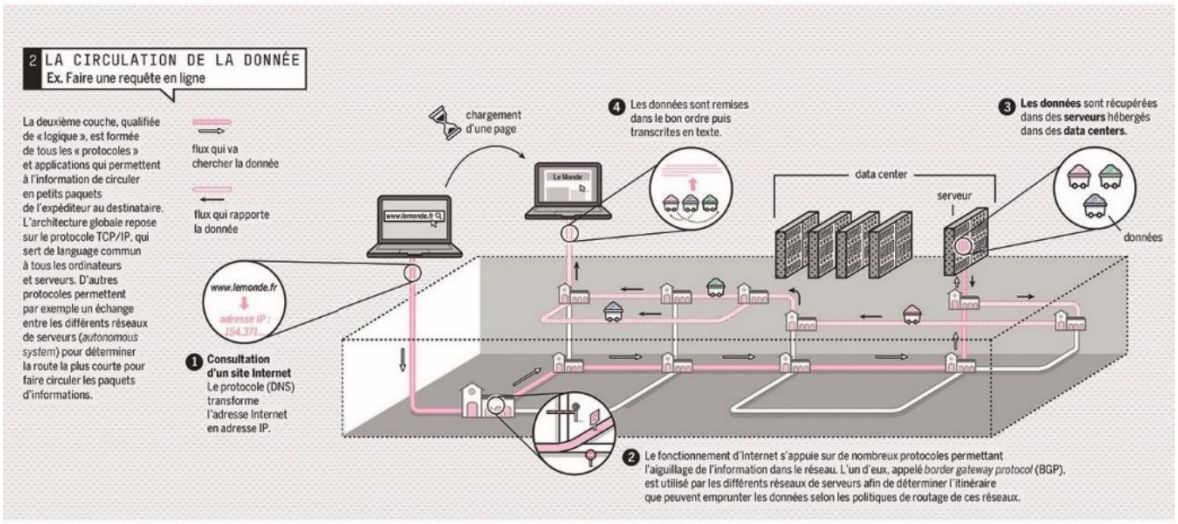



**Figure 4 :** *Schéma simplifié de la deuxième couche (logique)*

Source : « Le Cyberespace. un enjeu de géopolitique majeur », F. Douzet, *Le Monde*, 22-23/07/18.

Les protocoles sont incontournables et jouent le rôle de chefs d'orchestre. Par exemple, le protocole IP (*Internet Protocol*) permet d'aiguiller les *paquets* de données (couche 3-réseau du modèle OSI). Celui-ci est souvent associé au TCP (*Transmission Control Protocol* – couche 4-transport) qui se charge de transmettre et vérifier si tous les paquets, devenus *segments/datagrammes*, sont correctement acheminés vers une machine. UDP (*User Datagram Protocol*) est un autre protocole de transmission de données qui ne nécessite pas une connexion formalisée comme TCP (il est notamment utilisé dans le *streaming*). On peut

aussi citer le protocole HTTP (Web) ou le protocole d'infrastructures le DNS (*Domain Name System*) qui permet le nommage et assure la conversion entre langage binaire-machine (adresse IP) et le langage naturel humain (noms de domaine).

Le code est dit de haut niveau grâce à une standardisation des langages de programmation, ce qui permet la compatibilité d'instructions logicielles entre architectures matérielles disparates. Le code est vulnérable et dépend en partie d'un savoir-faire en programmation, toutefois des anomalies logicielles ou erreurs humaines sont inéluctables. Pour cette raison, les éditeurs corrigent leurs programmes et déploient régulièrement des mises à jour appelées correctifs ou « patchs ». La mise à niveau de ces logiciels est un des principes élémentaires de la sécurité informatique, et il incombe aux utilisateurs d'y procéder. Le code est à la fois la cible et l'arme qui l'attaque. Donc attaquer la couche logique consiste à identifier et exploiter les failles de sécurité logicielles. Or, ces vulnérabilités font l'objet d'un véritable marché noir où tous types d'acteurs réalisent des transactions pour en avoir la primeur. Les failles dites « zero-day » sont très recherchées y compris par des États. Ces vulnérabilités critiques sont dites « jour zéro » dans le sens où elles n'ont été identifiées que par quelques rares acteurs sans avoir été rendues publiques. Les éditeurs de logiciels et la quasi-totalité des utilisateurs y compris informaticiens en ignorent l'existence jusqu'au jour où elles sont exploitées, le plus souvent à des fins malveillantes par des cybercriminels, ou bien découvertes par des chercheurs en sécurité informatique. En 2017, le ransomware *Wannacry* a par exemple exploité une faille 0-day présente sur le système d'exploitation Windows de versions principales XP, 7, 8 et Vista. Cette faille avait été découverte par la NSA qui l'avait baptisée *EternalBlue* ainsi que l'*exploit*[96] permettant d'en profiter. Elle touchait un protocole de partage de ressources sur des réseaux locaux de PC Windows, le protocole SMB (*Server Message Block*, V.1.0) [97]. Or, cet *exploit* a été subtilisé par un groupe de hackers connu sous le nom de *Shadow Brokers*, qui pourrait être nord-coréen ou russe. Autrement dit, la NSA a cherché à identifier des failles sur l'OS Windows pendant un an avant de détecter ce qui deviendra *EternalBlue*, l'exploitant durant cinq ans, puis a été piratée par lesdits hackers qui l'ont publicisée (sur *Twitter*) et exploitée pour déployer *Wannacry*. **La ruse le dispute bien à la force**. Microsoft apprendra l'existence de cette faille sur son système après le piratage de la NSA, en mars 2017, un mois seulement avant le déploiement du rançongiciel. Malgré la publication rapide d'un correctif, des centaines de milliers d'ordinateurs seront touchés car non mis à jour. De même et plus récemment, le

[96] Un *exploit* (prononcé à l'anglaise) désigne toute technique permettant d'exploiter une faille de sécurité informatique. On peut trouver un équivalent de celui utilisé à l'époque par la propre NSA. Baptisé *DoublePulsar* (*https://www.rapid7.com/db/modules/exploit/windows/smb/doublepulsar_rce/*), il est notamment disponible et prêt à l'emploi (avec guide d'utilisation) sur un outil-cadre célèbre dans le *pentesting* et appelé *Metasploit*. Il s'agit d'un *framework* de développement et exécution d'*exploits* (https://www.metasploit.com/). Cette faille permettait de récupérer les ressources de SMB via des *exécutions de code à distance* (RCE).

[97] https://www.avast.com/fr-fr/c-eternalblue

logiciel d'espionnage Pegasus, édité par la société israélienne NSO Group, a notamment exploité une faille *0-day* de l'application SMS *iMessage*, installée nativement dans l'iOS des *smartphones* Apple. La marque à la pomme ignorait l'existence de cette vulnérabilité.

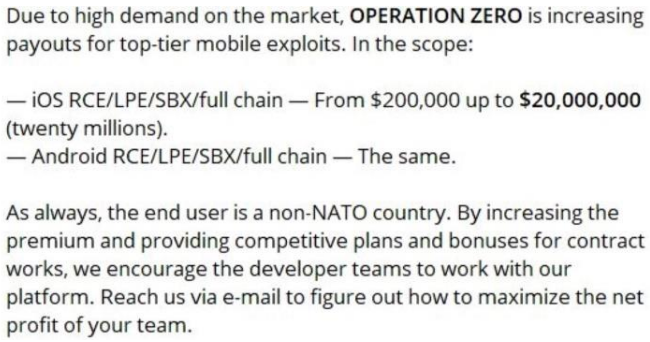
Ainsi, des États autoritaires ou démocratiques peuvent être tentés non seulement d'identifier des *0-day* et de concevoir les *exploits* associés à des cybercriminels, mais ils peuvent aussi les acheter auprès de ces derniers. Le *New York Times* a rapporté le cas d'une vulnérabilité qui aurait été monnayée à hauteur de 500 000$ dont l'acquéreur serait vraisemblablement une entité étatique, non déterminée[98]. L'objectif de ces États est de se réserver l'exclusivité d'une telle découverte soit à des fins d'exploitation offensive ou de contre-mesure défensive, soit d'empêcher que d'autres entités ne puissent en bénéficier. Par ailleurs, des acteurs privés peuvent également prendre part à ces transactions : les éditeurs de logiciels bien sûr – quand ils en ont cependant les moyens – et en catimini, pour assurer la fiabilité *a posteriori* de leurs produits et ne souffrir aucune atteinte réputationnelle indirecte. Des entreprises moins bien-intentionnées peuvent les acheter pour constituer un arsenal, et certaines très particulières en ont fait un modèle économique tout à fait légal. Dans la veine de NSO Group, une telle société cette fois italienne, Hacking Team, exploite la recherche et éventuellement l'achat de ces failles pour rendre plus performants les outils offensifs (logiciels de surveillance) dont elle fait par ailleurs le commerce auprès d'États aux intentions malveillantes. Ou encore l'entreprise française montpellieraine Vupen, spécialisée dans la revente de vulnérabilités *0-day* et fondée par un Franco-Marocain du nom de Chaouki Bekrar. En 2004, il fonde donc Vupen qui, en France, est la première société à faire du *full disclosure*[99] sur ce type de failles, c'est-à-dire en faire la divulgation complète en dépit des retombées négatives évidentes[100]. Confrontée aux pressions de la Direction centrale du renseignement intérieur (DCRI*), à des lourdeurs administratives et des menaces de sanctions juridiques compte tenu du flou entourant son activité, Chaouki Bekrar décide de dissoudre l'entreprise en France mais de poursuivre son travail à partir de la filiale américaine qu'il avait créée pour la rebaptiser Zerodium. Celle-ci a signé des accords notamment avec la NSA pour devenir l'un des principaux fournisseurs de failles « jour-zéro » des États-Unis. Dans un autre contexte et le cadre des tensions russo-occidentales, la plateforme officielle russe *Opération Zéro* a publié en septembre 2023 un avis

[98] Rayna Stamboliyska, *op. cit.*, p. 43. Selon Victor Poucheret (entretien du 14/11/2021), l'État français peut possiblement compter parmi ces entités publiques.

[99] Comme son nom anglais l'indique, le *full disclosure* consiste à publier intégralement le détail d'une faille de sécurité. Beaucoup de hackers agissaient ainsi y compris à des fins bienveillantes pour alerter les éditeurs touchés et dans le même temps dénoncer véhément le manque de législation publique autour de la recherche de vulnérabilités. La pratique du *full disclosure* était et reste interdite en France, mais les systèmes de *bug bounty* sont venues réguler et « privatiser » les remontées de failles (en France à partir de 2016).

[100] Entretien avec Jean-Marc Manach, 10/04/2023.

de récompense pouvant s'élever à 20M$ pour toute remontée de faille critique sur les systèmes Android et iOS.



Due to high demand on the market, **OPERATION ZERO** is increasing payouts for top-tier mobile exploits. In the scope:

— iOS RCE/LPE/SBX/full chain — From $200,000 up to **$20,000,000** (twenty millions).
— Android RCE/LPE/SBX/full chain — The same.

As always, the end user is a non-NATO country. By increasing the premium and providing competitive plans and bonuses for contract works, we encourage the developer teams to work with our platform. Reach us via e-mail to figure out how to maximize the net profit of your team.

**Figure 5 :** *Capture d'écran dudit avis posté sur LinkedIn par Clément Domingo*

Source : *https://fr.linkedin.com/in/clementdomingo*

Enfin, autre exemple paraissant plus terre à terre, des entreprises comme Cdiscount peuvent assurer à leurs RSSI/*red teams* la liberté d'aller faire de la reconnaissance en naviguant sur le *darkweb* (pour appréhender la créativité en termes de techniques de fraude) ou visiter des sites spécialisés y compris le web classique « *où les brokers revendent des infos et par exemple sur les failles zero-day qui s'achètent, par des entreprises notamment*.[101] »

Les failles logicielles, qui forment donc l'enjeu central de la deuxième couche du cyberespace, génèrent des problèmes juridiques complexes par un manque délibéré de régulation, à l'image des activités d'espionnage plus généralement. Cela pose la question des usages duaux des technologies numériques, lesquelles peuvent être arsenalisées et devenir des outils offensifs, mais pour autant constituer également un enjeu d'intérêt public. Les chercheurs en cybersécurité et les hackers légaux contribuent à faire de la recherche et développement sur les vulnérabilités informatiques, les plateformes légales de *bug bounty* comme en France YesWeHAck et Yogosha participent à une activité ambiguë[102] mais finalement dans le même temps nécessaire pour renforcer la sécurité numérique dans son ensemble. « *La loi française est très stricte,* souligne Guillaume Poupard, *donc un chercheur en informatique est toujours*

[101] Entretien avec Damien Cazenave, 24/07/2017. Un site comme raidforums.com était présent sur le web surfacique. Il a été saisi par Interpol et le FBI en 2022 (https://raidforums.com/ ; https://web.archive.org/web/20220130171918/https://raidforums.com/Announcement-Database-Index-CLICK-ME). Le site hackforums.net, toujours actif et proposant entre autres des formations/tutoriels « *Black Hat* », est également assez litigieux mais ne propose *a priori* pas de bases de données « leakées » (https://hackforums.net/). Fait curieux, Cdiscount recrute des hackers (notamment à l'étranger pour cause de concurrence et de moindre niveau à Paris), constitue des pools de *red*/*blue teamers* mais n'a, à ce jour, toujours pas implémenté de 2nd facteur d'authentification en faveur de ses clients sur son site web.
[102] Entretien avec Frédérick Douzet, 30/03/2022.

*limité. Car un hacker, ce n'est pas un blanc "pur"*.[103] » À l'instar des logiques de l'*open source* précédemment évoquées, la cybersécurité mêle deux approches différentes, complémentaires et engendrant des externalités négatives : la sécurité dite « par l'obscurité » consiste, notamment pour les éditeurs de logiciels à ne pas publier leur code source pour des raisons évidentes (mais rarement justifiées) en dissimulant éventuellement en connaissance de cause ou en ignorant de bonne foi les propres vulnérabilités de leurs produits Dans ce cas de figure, les utilisateurs doivent faire confiance aux éditeurs, sans possibilité de vérifier efficacement par eux-mêmes. Par ailleurs, les tenants du principe de la sécurité dite « par la transparence » militent *a contrario* pour la publication systématique des codes sources afin de pouvoir aider et mutualiser le travail de recherche sur les failles, afin d'en assurer la publication et donc la correction le plus rapidement possible. **La confiance est ici plus de mise puisqu'il est possible de soumettre les logiciels à des audits. L'inconvénient est que si tout le monde est en capacité de le faire, alors des acteurs malveillants le peuvent également. Or, certains d'entre eux sont dédiés à cette recherche et jouissent par ailleurs d'un très haut niveau technique, ils seront donc potentiellement plus agiles et à même d'exploiter les brèches**.

Au-delà de ces aspects liés aux vulnérabilités informatiques, il convient de mentionner brièvement l'emprise qu'exercent sur cette couche du cyberespace les entreprises numériques, en particulier les GAMAM* et dans leur sillage les BATHX[104]. Citons notamment la recherche & développement considérable investie ou puisée dans les sciences cognitives et l'exploitation des biais éponymes pour servir l'économie de l'attention[105] ou ce qui est qualifié de *capitalisme de surveillance*. Mentionnons l'inventeur de cette *captologie*, le sociologue américain Brian J. Fogg et son célèbre *Persuasive Technology: Using Computers to Change What We Think and Do*[106]. La seule question des techniques appelées *dark patterns* est significative des pratiques de ruse voire de vice que peuvent mettre en œuvre de tels acteurs. Ces « designs déceptifs » consistent en des interfaces utilisateurs disposant des mini-pièges cognitifs au gré de la navigation de l'usager[107]. Sans parler de l'algorithmique mise à contribution pour manipuler l'attention des usagers par la préemption des contenus viraux, exploiter leurs biais cognitifs et optimiser la rentabilité des plateformes de médias sociaux. D'une manière générale, comme

[103] Entretien avec l'auteur, 17/04/2023.

[104] L'acronyme GAMAM vient remplacer celui de GAFAM depuis que Facebook est devenu le groupe Meta en 2021. Les sociétés chinoises Baidu, Alibaba, Tencent, Huawei et Xiaomi. Et ajoutons ByteDance (TikTok/Douyin).

[105] Bruno Patino, *La civilisation du poisson rouge : Petit traité sur le marché de l'attention*, Grasset, 2019, 184 p.

[106] Brian J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, 2003, 312 p.

[107] Par exemple, une assurance cochée par défaut, un bouton de non-consentement au dépôt de cookies relégué au second plan ou dans un sens de lecture non conforme aux codes culturels de l'utilisateur, *nudges* via les couleurs, téléchargement non désiré de briques logicielles, messages faisant pression sur le consommateur pour favoriser l'achat…

outils de communication, ces derniers exercent une influence tout à fait réelle sur nos comportements et nos manières de penser. Quel rapport la France et les Français entretiennent-ils avec ces *géants* du *numérique* ? À en croire le lieutenant-colonel de gendarmerie Laurent Leberon : « […] *Le problème en France, c'est l'américanisation de la société.*[108] »

Au bilan, la couche logique est le niveau où se déroule à bas bruit, entre force et ruse, une *guerre informatique*. Les arme dites « numériques » sont une nouveauté complète dans l'histoire puisque c'est le code qui les a rendues possibles à développer et utiliser. On voit bien à quel point, en outre, elle pose des enjeux juridiques et politiques saillants, dès lors que c'est à ce niveau que les normes de « gouvernance » peuvent être établies, étant entendu que celles-ci sont l'objet de tensions entre les nombreux acteurs en capacité de les édicter, dans une logique similaire à l'anarchie qui caractérise les relations internationales. Bien entendu, l'usage de « l'intelligence artificielle » va complexifier ces enjeux, tout comme l'opacité algorithmique engendre déjà des dérives dans la manipulation du code et l'interprétation du réel. *In fine* se pose la question de la « neutralité du Net[109] » ou plus exactement encore de celle du Web, puisqu'au-delà des FAI qui peuvent créer un internet à plusieurs vitesses, ce sont surtout les *géants du numérique* qui présentent, filtrent, et donc façonnent l'information et les perceptions sur le Web. Il est toujours édifiant de constater les mesures de contrôle de temps d'usage imposées par l'État chinois à ses utilisateurs de réseaux socionumériques comme TikTok ou encore d'entendre les ingénieurs des GAMAM dire que ce qu'ils inventent pour le grand public sont des objets débilitants et que leurs propres « *enfants ne sont pas autorisés à utiliser cette merde.*[110] » Si, comme le dit la spécialiste Aurélie Jean, l'algorithme n'est pas neutre, alors au-delà d'une guerre informatique se joue une guerre cognitive qui s'articule parfaitement avec la troisième et dernière couche du cyberespace.

- *La troisième couche est la couche sémantique. Elle forme une sphère informationnelle où règne l'influence.*

Cette dernière strate est également désignée comme la couche socio-cognitive ou encore humaine. On y produit donc de la socialisation, du sens et de la connaissance par mobilisation de processus mentaux ; elle est la plus visible et prégnante pour l'humain qui peut y mobiliser son langage dit naturel, que traduira la couche inférieure grâce à ses logiciels, lesquels traduiront à leur tour leurs langages de programmation à la couche la plus basse, celle du langage-machine. C'est ainsi qu'elle est considérée comme la *couche haute* de l'espace

[108] Entretien avec l'auteur, 21/06/2017.
[109] Sur cette question, voir Stéphane Bortzmeyer, *op. cit.*, pp. 235-247.
[110] Mots prononcés par un ancien haut cadre de Facebook, Chamath Palihapitiya.

numérique. On se situe ici dans ce qu'il est convenu d'appeler les *contenus*, acheminés par les *contenants* que regroupent les couches basses précitées.


**Figure 6 :** *Schéma simplifié de la troisième couche (sémantique)*

Source : « Le Cyberespace. un enjeu de géopolitique majeur », F. Douzet, *Le Monde*, 22-23/07/18.

Elle est bien évidemment la raison d'être du cyberespace puisqu'elle permet d'inter-relier les individus en faisant fi des distances physiques, et de leur proposer des services numériques dans de nombreux domaines. En somme, cette strate représente le but alors que les couches basses en constituent le moyen. Finalement, dans la perspective de l'histoire de l'humanité, si brillamment synthétisée par Yuval Noah Harari dans son *Sapiens*, le cyberespace à travers sa troisième couche est une sorte d'aboutissement de l'évolution par l'aptitude de l'humain à collaborer ou plus largement socialiser grâce à la communication. C'est donc presque exclusivement par la ruse et la création ou l'altération de l'information que l'on va exercer une influence et ainsi exploiter cette couche ; ce que l'on apparente aux *guerres de l'information* : opérations psychologiques (*PsyOps*) ; ingénierie sociale (où excellent les hackers) ; désinformation ; mésinformation, intoxication ; mystification ; déception ; propagande ; manipulation ; censure et rétention ; *agnotologie*[111]… Rien de nouveau en somme dans la conflictualité immatérielle, mais la problématique et la pratique sont démultipliées et *augmentées* par les effets instantanés, viraux, réticulaires et de levier des technologies de

[111] L'*agnotologie* peut se résumer dans la citation de Victor Hugo : « *L'ignorance est la nuit qui commence l'abîme.* » Néologisme inventé par l'historien des sciences (Stanford) Robert N. Proctor*, Agnotology: The Making and Unmaking of Ignorance*, 1st, 2008, 308 p., l'agnotologie désigne l'étude des diverses formes de l'ignorance et, en particulier, la manière dont la société la produit, l'entretient ou la propage.

l'information et de la communication (TIC*). L'information était considérée plutôt comme un moyen notamment militaire (guerre réseau-centrique) de maîtrise du combat (espionnage, tactique) cependant qu'elle est devenue un champ de conflictualité en soi, traversant toutes les sphères d'activités humaines et ainsi élargi à l'ensemble de la société.

| Procédés | Mode d'action |
|---|---|
| ***Communication*** | Information |
| | Argumentation |
| | Suggestion |
| | Persuasion |
| | Obédience |
| ***Mystification*** | Stratagème |
| | Déception |
| | Intoxication |
| | Désinformation |
| ***Aliénation*** | Propagande |
| | Endoctrinement |
| | Subversion |
| | Terrorisme |
| ***Protection*** | Contre-information |
| | Contre-propagande |
| | Dépersuasion |

**Figure 7 :** *Procédés et modes d'action sur la couche sémantique*

Source : Bertrand Boyer, *Cybertactique*, *op. cit.*, pp. 112-113.

Les impacts de ces pratiques d'altération de l'information à des fins politiques, idéologiques, militaires ou encore sociétales sont encore très sous-estimés, bien qu'on commence à prendre la mesure du danger dès lors qu'on s'intéresse aux applications et implications de l'IA dans le domaine. Des montages techniques comme les *deep fakes*[112] sont la parfaite – et vraisemblablement préalable – illustration de ce qu'il est possible de faire pour semer la

[112] Les *deep(learning) fakes* ou « hypertrucages » désignent un ensemble de techniques de fusion de ressources multimédia en vue de synthétiser des contenus numériques par IA. Il s'agit par exemple de faire prêter des propos fictifs mais perçus comme réels (synchronisations labiale, image/son) à une personnalité publique.

confusion au sein des populations. Les avancées algorithmiques déjà particulièrement manipulatoires sur les RSN aux seules finalités commerciales et marketing d'entreprises privées pourraient augurer d'opérations politiques de manipulation de masse sans précédents dans l'histoire. Des plateformes numériques tenant parfois dans des « super-applications » concentrant les activités quotidiennes d'ordre récréatif, professionnel, économique et social des utilisateurs pourraient conduire à des enfermements cognitifs particulièrement néfastes y compris pour la « santé mentale publique ». Certains prospectivistes ne disent pas autre chose quand ils établissent des scénarii où la dynamique de *post-vérité* pourrait devenir la norme et générer des perceptions de réalités parallèles, à travers des bulles cognitives communautaires pouvant générer des situations de totale acommunication. À la « balkanisation » territoriale et politique succèderait alors une *balkanisation sociocognitive*[113].

Plus proche de notre réalité présente, l'émulation créée par la concurrence acharnée entre sociétés numériques comme Meta et ByteDance montre désormais que les plateformes de médias sociaux américaines, jusqu'ici dominatrices, s'inspirent voire copient les innovations algorithmiques de l'application *TikTok*, tandis qu'Elon Musk, nouveau patron de *Twitter* et désormais *X*, lorgne du côté du chinois Tencent et de sa « superapp » WeChat/Wēixìn, qui concentre et centralise des fonctionnalités de réseau social, messagerie instantanée, plateforme de paiement (type Paypal) et accessoirement cheval de Troie/système de surveillance globale des usagers chinois aux mains du Parti communiste. *TikTok* est par ailleurs régulièrement accusé d'utiliser un algorithme très puissant en termes d'addiction numérique et sa version native chinoise (*Douyin*) est d'ailleurs bien plus contrôlée et censurée. Bien plus, *Tiktok* – et ses futurs épigones – serait envisagé par le régime comme, d'une part, un moyen de damer le pion à la concurrence américaine jusqu'ici intouchable, d'autre part tel un instrument de guerre cognitive et de subversion offrant une telle liberté de production et diffusion de contenus qu'elle constituerait un instrument de *soft* (*TikTok* est devenu un des RSN les plus utilisés chez les jeunes, plus malléables[114]) et *sharp power* (*shadow banning*[115])

[113] https://www.defense.gouv.fr/aid/actualites/red-team-defense-devoile-ses-nouveaux-scenarii-menaces-conflictualites. « Red Team », *Ces guerres qui nous attendent : 2030-2060*, Des Équateurs, 2022, 222 p. La Red Team est la très sérieuse cellule d'analyse prospective mise en place au sein du MINARM et réunissant auteurs de science-fiction et dessinateurs. Elle confronte ses projections à une Blue Team modératrice composée d'officiers, d'ingénieurs et analystes. L'analogie terminologique et bichromique conférant aux équipes de hackers-attaquants/informaticiens cybersécurité-défenseurs est tout à fait intéressante.

[114] https://www.blogdumoderateur.com/etude-adolescents-utilisent-tiktok-facebook/

[115] L'algorithme de *TikTok* censurerait ou relèguerait furtivement les contenus non conformes aux valeurs chinoises. Or, cet algorithme se singularise par la mise en avant des contenus les plus viraux et non les producteurs de ceux-ci. Cette particularité, qui réinvente l'approche classique des RSN américains, égalise les statuts sociaux et permet à n'importe quel usager de connaître son quart d'heure de gloire (un contenu populaire succédant très rapidement à un autre, rendant leur popularité, et ainsi leur auteur, tout à fait éphémère). Voir notamment le rapport intitulé *La tactique TikTok : opacité, addiction et ombres chinoises* (https://www.senat.fr/rap/r22-831-1/r22-831-1_mono.html) et Jean-Baptiste Jeangène Vilmer & Paul Charon, *Les opérations d'influence chinoises. Un moment machiavélien*, IRSEM, 2021, 654 p.

pour le pouvoir chinois. À savoir, en mesure de semer les graines d'idées questionnant les valeurs occidentales en exploitant habilement la permissivité du droit d'expression et des libertés au sens large qui caractérisent nos démocraties.

Nous ne détaillerons pas par le menu la déjà très documentée question des GAMAM/NATU*[116], firmes technologiques systémiques dont les dirigeants revendiquent implicitement le statut d'acteurs supranationaux quand elles perturbent déjà grandement les États traditionnels par leurs dynamiques transnationales. L'effet de loupe créé par leur position monopolistique sur une activité emblématique (moteur de recherche pour Google, voitures électriques chez Tesla, marché de e-commerce avec Amazon…) masque largement aux yeux du grand public une vocation globale sinon totale. « *Un positionnement qui leur permet de se façonner une image d'organisations quasi philanthropiques avec des engagements progressistes, d'affirmer leur puissance et de faire oublier que leur pouvoir repose sur l'exploitation des données personnelles des 5 milliards d'internautes dans le monde.*[117] »

De la même manière, ne sera pas étudié ici le sujet de « l'Internet caché » ou « illégal » tel qu'il est souvent présenté dans une dramaturgie toute médiatique. Les *darknets/darkwebs*, puisqu'il s'agit de cela, ne sont que des réseaux superposés (*overlay networks*) qui forment des ressources numériques difficiles à quantifier – au-delà des stéréotypes liés à l'analogie de l'iceberg immergé. Un *darknet* est un réseau physique très décentralisé (relation de pair à pair – P2P) que constituent des machines (serveurs, ordinateurs…) appartenant généralement à des particuliers. Ce sont des réseaux d'ordinateurs alternatifs à l'Internet public mondial. Parmi ces réseaux superposés, on compte par exemple les services de voix sur IP (VoIP). Le plus connu est celui de l'OnionLand ; le réseau logique associé et donc le web afférent à ce *darknet* est un *darkweb*, appelé en l'espèce TOR (*The Onion Router*). Il est nécessaire d'utiliser un navigateur web dédié à ces réseaux physique/logique. TOR nécessite par exemple le navigateur éponyme fondé sur une déclinaison de Firefox, le logiciel créé par l'ONG Mozilla. Il existe d'autres *darknets*/*darwebs* comme Freenet (le plus ancien – 2000) ou I2P (*Invisible Internet Project*). Certains sont dits mixtes et permettent de naviguer à la fois sur le Web *visible* (donc grâce à l'Internet public mondial) et un *darkweb* ; c'est le cas de TOR[118]. Ces espaces

[116] L'acronyme NATU, pour Netflix, Airbnb, Tesla et Uber, désigne d'autres *Big Tech* états-unienne à vocation globale. Du reste, la marque Google oblitère la firme Alphabet qui évolue dans nombre de secteurs technologiques (Google Calico/Waymo/Nest/Fiber, téléphonie avec Nexus et Pixel…)

[117] Julien Nocetti, « Des acteurs systémiques ? Les GAFAM au centre des jeux internationaux », in Stéphane Taillat, Amaël Cattaruzza, Didier Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2023, 288 p., pp. 174-181.

[118] Toutes ces expressions (*darknet/darkweb*, *deep web* aussi, qui lui correspond simplement aux contenus du Web classique non indexés par les moteurs de recherche) relèvent plus d'éléments de langage qui, s'ils sont utiles, n'ont guère de sens du point de vue de l'informatique. Comme le dit Cédric Perrin (entretien du 05/10/2017), tout est une question de protocoles de communication entre infrastructures *hardware*, machines, serveurs, etc. Voir https://web.archive.org/web/20150325025545/http://darknet.se/about-darknet/ et

numériques superposés ne sont pas consacrés aux activités illégales, contrairement aux poncifs véhiculés. Ils sont aussi utilisés par des dissidents politiques de régimes autoritaires, des journalistes, des hackers et militants des libertés publiques et de la vie privée, mais aussi des services de renseignement ou de sécurité, cette fois pour lutter contre la cybercriminalité en particulier. Ou plus prosaïquement par n'importe qui souhaitant un maximum de confidentialité. La métaphore de l'oignon est tirée de ce que les dispositifs de chiffrement sont nombreux et encapsulés, permettant d'assurer un certain mais relatif anonymat (adresses IP masquées). Beaucoup de débats entourent les *darkwebs* et notamment TOR car il est le plus populaire, surtout en ce qui concerne la véritable fiabilité de ce réseau[119].

**Cette présentation simplifiée et compartimentée du cyberespace ne doit pas faire oublier que si ce dernier peut faire l'objet d'attaques sur une strate spécifique, la plupart des offensives touchent ou ont presque invariablement un impact sur les deux autres**. Citons, pour l'anecdote, le cas du spationaute (couche 3) porteur d'une clé USB (couche 1) qui aurait sans le savoir introduit un ver informatique (couche 2) dans le SI de la Station spatiale internationale (ISS) en 2008[120]. Ou encore la plus sérieuse et première du genre attaque cyber-physique *Stuxnet*, qui a visé les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz en Iran. Cette mission d'une opération de grande envergure baptisée « *Olympic Games* » a été décidée sous le mandat de George W. Bush, poursuivie et mise à exécution par Barack Obama en 2010. *Stuxnet* est un ver informatique en toute vraisemblance conçu conjointement par la NSA et l'unité 8.200 de Tsahal[121]. La plupart des sources concordent quant au vecteur de l'attaque : une clé USB (couche 1, périphérique) contenant le ver (couche 2, arme numérique) et introduite (*USB drop attack*, ingénierie sociale *VS* humains) auprès de fournisseurs ou prestataires (couche 3) de la centrale nucléaire iranienne, et son utilisation ultérieure sur le SI (couche 1, et 2 : manipulation de code ou contournement/*bypassing* de dispositifs de sécurité – certificats cryptographiques, élévation de privilèges administrateurs…) par les ingénieurs ou les techniciens (couche 3). Résultat, en attaquant numériquement les systèmes instrumentés de sécurité de la centrale, le ver provoque l'explosion concrète (environnement physique) d'un millier de centrifugeuses[122]. Autre

https://web.archive.org/web/20171215141104/http://www.cs.virginia.edu/~cs757/slidespdf/757-09-overlay.pdf

[119] On le doit en effet, à l'origine, à la Marine de guerre américaine. Voir https://www.torproject.org/fr/about/history/, et pour plus de détails sur les *darkwebs*, Rayna Stambolyiska, *op. cit.*, pp. 283-395. Ex-officier cryptologue de la DGSE, Éric Filiol dit avoir découvert dès 2012 que plusieurs administrateurs de TOR étaient liés à la NSA (http://www.lexpress.mu/news/920-interview-eric-filiol-expert-francais-en-securite-informatique.html).

[120] https://www.zdnet.fr/actualites/la-station-spatiale-internationale-infectee-par-un-virus-39382888.htm

[121] L'unité 8.200 est la cellule spécialisée dans la lutte informatique offensive de l'armée israélienne. Sur le détail de l'opération, voir par ex. https://www.youtube.com/watch?v=j-cv_YXg4Ps, vidéo publiée par une entreprise de cybersécurité française.

[122] En fin de partie 2 sera étudiée par le menu une attaque du même type.

exemple, les offensives informatiques et informationnelles réputées russes contre les États-Unis lors de l'élection présidentielle : prépositionnement de codes maliciels (couche 2) sur des infrastructures énergétiques/électriques (couche 1), piratage de la messagerie (couche 2) de l'équipe de campagne d'Hillary Clinton, et microciblage des électeurs américains par l'entreprise Cambridge Analytica sur les RSN (couche 3) au service du candidat républicain, Donal Trump[123]. Enfin, mentionnons l'affaire « Team Jorge » du nom d'une société israélienne dédiée au hacking, à la manipulation de l'information et à la militarisation des réseaux socionumériques. Infiltrée par trois journalistes dont un de Radio France, cette officine privée a été confondue pour ses activités d'influence dans le processus électoral de dizaines d'États africains, à la demande d'élus politiques locaux. La Team Jorge, du pseudonyme de son dirigeant, a eu partie liée avec la firme Cambridge Analytica aujourd'hui dissoute pour qui elle a assuré des missions de sous-traitance. Coordonnée par le consortium d'organes de journalisme d'investigation Forbidden Stories, l'enquête a révélé les *modi operandi* de l'officine israélienne. Elle proposait notamment le piratage de comptes Telegram et surtout l'emploi de faux profils de RSN générés et animés par des robots, le tout piloté par une plateforme d'IA baptisée AIMS (*Advanced Impact Media Solutions*). Cette dernière concevait de manière semi-automatique des narratifs pour ces avatars afin d'instrumentaliser les débats autour de trente-trois élections présidentielles africaines dont vingt-sept auraient été manipulées avec succès, menant à la victoire les clients de la Team Jorge[124].

Comme le soulignent Raphaël Chauvancy et Rayna Stambolyiska en des termes différents mais convergents, l'espace informationnel/le cyber vient oblitérer les frontières et les certitudes. Les cybermenaces induisent un amalgame entre intérieur et extérieur, défense et sécurité en réduisant la sécurité collective au profit d'une sécurité individuelle[125]. Il conforte le retour à l'unilatéralisme des États et alimente la compétition globale entre différents acteurs, publics et privés, individuels et groupaux, en égalisant leur pouvoir. La guerre devient permanente et ne correspond plus à une séquence définie et claire. L'époque se caractérise par une extension du domaine de la conflictualité et l'extra-militarisation de la guerre[126]. Le cyberespace y contribue drastiquement, autorisant guerres hybrides et cognitives. Ainsi implique et nourrit-il une dialectique de la force (contenants, attaques informatiques) et de la ruse (contenus, offensives informationnelles) pour en faire le véhicule du « crime parfait », banalisé, imperceptible. Au bout du compte, l'espace numérique *augmente* les niveaux et dimensions de la stratégie–opératique–tactique–logistique–technologie (systèmes d'armes) en les unissant comme ils ne l'ont jamais été. En atteste la notion militaire consacrée et

[123] De même, cette opération sera détaillée en partie 2.
[124] https://forbiddenstories.org/fr/story-killers/team-jorge-desinformation/
[125] Rayna Stambolyiska, *op. cit.*, pp. 119-123.
[126] Raphaël Chauvancy, *Les nouveaux visages de la guerre*, VA, 2023 (2e éd.), 270 p., p. 18.

aisément transposable au civil de « caporal stratégique », notamment à travers les logiques de *médiactivisme*, *hacktivisme*, *ego-activisme ou encore iCTIvisme*[127]. Toute action individuelle de niveau tactique peut avoir un impact stratégique. Ainsi, le Web *social* notamment engendre des externalités difficiles à anticiper ou à contrer. Par exemple, un soldat du rang ou sous-officier, en l'occurrence ici et en 2003 un caporal des US Marines avait drapé la statue déchue de Saddam Hussein d'une bannière étoilée. Avant qu'un officier supérieur lui enjoigne de la retirer, une photo a immortalisé l'évènement en faisant le tour du monde par le truchement des réseaux socionumériques. L'image originelle de soldats libérateurs va alors imperceptiblement glisser vers celle d'une armée d'occupation. Si la portée du concept est à relativiser, il est toutefois représentatif du phénomène des luttes d'influence favorisé par la mise en réseau numérique des activités humaines. Les ONG ou des individus, par exemple, parviennent à faire basculer des opinions publiques par l'effet de levier qu'ils tirent de leur activisme numérique.

« *Kubernetes* », rappelle Olivier Kempf, signifie aussi « doué pour le mouvement »[128]. Ainsi, dans le cyberespace, *l'agilité des uns fait la paralysie des autres*[129]. La prime sur ce milieu revient donc aux pro-acteurs qui savent en exploiter les singularités, souvent résumées par l'acronyme anglosaxon « VUCA » : *volatil(e)*, *i(u)ncertain*, *complexe* et *ambigu*.

| **Caractéristiques du cyberspace** | **Implications** |
|---|---|
| Complexité, ambiguïté, instabilité | Difficile à appréhender, impossible à maîtriser |
| Volatilité et imprédictibilité | Difficile à préhender, mesurer, et investir |
| Ubiquité et transversalité | « Bouillard de guerre », actions peu localisables |
| Virtualité/évanescence et réversibilité/résilience | Mise en abime réticulaire, dommages réparables |
| Asymétrie et égalisation | Modifie et/ou égalise les rapports de puissance |
| Réticularité et massivité | Augmente les effets de levier/de masse/bascule |
| **Armes numériques (critères)** | **Caractéristiques** |
| Portée | « Universalité », liée aux réseaux |
| Vitesse | Instantanéité des effets, ± longue préparation |
| Puissance | Relativité, ambivalence du seuil de la guerre |
| Précision | Attaques microciblées « chirurgicales » |
| Discrétion | Furtivité & dissimulation, attribution délicate |
| Accessibilité | Bon rapport coût/efficacité, pouvoir égalisateur |

**Figure 8 :** *Caractéristiques et implications du cyberespace et des armes numériques*

Source : Yannick Pech, 2023.

[127] Emmanuel Bloch, *Communication de conflictualité et mouvements activistes sur Internet (2006-2011),* thèse de doctorat en sciences de l'information-communication, université Paris II – Panthéon Assas, 2016, pp. 54-103.
[128] Olivier Kempf, *Introduction à la cyberstratégie*, Economica, 2012, 176 p.
[129] Formule consacrée issue des travaux de Nicolas Moinet.

Ainsi, comme le souligne très justement l'expert en SSI Marc Sejean : **« *Tant en hard power qu'en soft power, le hacker est devenu le bras armé invisible des États-nations*.[130] » Entre force insaisissable et ruse imperceptible, le cyberespace permet donc à tous types d'acteurs de se livrer une compétition globale : firmes technologiques concurrençant par leur capacité financière et leur influence des acteurs étatiques, cybercriminels fragilisant l'économie légale ou encore entités politiques cherchant à se déstabiliser mutuellement**. Pour les États, qu'elles soient réalisées sous faux drapeau ou *proxies*, les opérations cyber sont un moyen pour contourner les garde-fous qu'ils se sont eux-mêmes imposés dans l'exercice de la force létale. *Fermez la porte à la guerre, elle passera par la fenêtre* pourrait-on dire. Ainsi, bien en peine d'en maîtriser le cours, le fonctionnement et les codes, les États ont depuis les années 2000 développé des législations de sécurité *du* numérique visant à en encadrer les pratiques, protéger les actifs critiques et lutter contre les menaces diffuses qui se multiplient dans le cyberespace.

[130] Entretien avec l'auteur, 20/03/2023.

## **B.** *Les politiques de sécurité du numérique*

Dans le cadre du Forum international de la cybersécurité (FIC*) de 2019, le directeur de l'Agence nationale des systèmes d'information (ANSSI*) a appelé tous les acteurs de l'écosystème numérique à prendre leur part de responsabilité dans la sécurité pour stabiliser le cyberespace : « *Ces dernières années nous ont montré l'importance capitale du rôle que doivent jouer les acteurs privés, publics et la société civile. C'est en travaillant collectivement, que nous pourrons stabiliser le cyberespace et éviter la structuration d'un* farwest *numérique.*[131] » Née en 2009, l'ANSSI assure une mission d'autorité nationale en matière de cybersécurité et de cyberdéfense tout en animant l'écosystème numérique. Elle forme ainsi la pierre angulaire de la sécurité numérique du pays. Son pendant militaire est le Commandement de cyberdéfense (COMCYBER*), qui est en charge de la SSI du ministère des Armées (MINARM*, hors DGSE* et DRSD*) et responsable des opérations militaires de cyberdéfense, en dehors des activités propres de la Direction générale de la sécurité extérieure (DGSE), indépendante.

De son côté, le ministère de la Justice développe sa politique de sécurité numérique. Quant au ministère de l'Intérieur (MININT*) il envisage – en 2023 – la création de son propre « COMCYBER-MI »[132] en s'inspirant du COMCYBERGEND* de la gendarmerie nationale – à moins qu'il ne s'agisse d'une fusion-réorganisation. Cette simple esquisse d'une description organisationnelle montre déjà à ce stade que le sujet de la cybersécurité a certes été pris à bras le corps, mais dénote une difficulté à unifier d'une part les administrations publiques, d'autre part toutes les forces vives du pays. Depuis plus de dix ans plusieurs documents sont venus enrichir la réflexion et impulser des politiques de sécurité et de défense liées à l'espace numérique. Or, on n'y trouve aucune mention de la possibilité d'employer des hackers légaux pour soutenir l'effort en termes de sécurité. Nous voulons ici succinctement passer en revue ces différents textes et interroger la question d'un possible emploi de tels profils au sein du dispositif national de cybersécurité.

[131] https://www.ssi.gouv.fr/actualite/fic-2019-lanssi-appelle-a-un-engagement-collectif-pour-stabiliser-le-cyberespace/

[132] https://www.senat.fr/basile/visio.do?id=qSEQ220700681&idtable=q397252|q417232&_c=%22parquet+national+cyber%22&rch=gs&de=20030909&au=20230909&rqg=drqscpt&dp=20+ans&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn

### 1) Généalogie critique de la cybersécurité nationale

En France a été fait le choix sémantique de parler de *sécurité des systèmes d'information* avant de reprendre, rarement toutefois dans les textes officiels, le terme courant de *cybersécurité*. De même, la notion de cyberespace a été supplanté par l'expression d'espace numérique, jusqu'à amalgamer SSI et non pas *sécurité numérique* mais *sécurité* du *numérique*. Ces hésitations témoignent d'une première chose : les systèmes d'information sont avant tout des systèmes informatiques. Ce qui dénote, d'une part, une vision proto-militaire et juridique, donc rationaliste, puis, d'autre part, une approche moins humaine et donc plus technique du sujet. Rappelons la définition donnée par l'ANSSI : « *espace de communication constitué par l'interconnexion mondiale d'équipement de traitement automatisé des données numériques*. » Or, comme l'indique justement Jean-Louis Gergorin et Léo Isaac-Dognin :

> « *On a longtemps considéré, dans le monde occidental, que ce qui importait était les deux premières couches, à savoir l'infrastructure matérielle et les logiciels. Car il n'y a pas à regarder le contenu : dans une démocratie, ce qui est dit n'a pas à être régulé. On s'intéresse donc surtout à l'infrastructure et aux logiciels. Et, en général, les agences de cybersécurité occidentales, en France par exemple, se sont structurées ainsi, en se concentrant sur les deux premières couches*.[133] »

En revanche, de l'autre côté de l'Atlantique, on a d'emblée privilégié le domaine global de l'information (*Information Warfare*). Tandis qu'en Russie, la notion de « sphère informationnelle » intègre les trois couches cyber et fusionne champs matériels et immatériels dans une seule et même approche stratégique (*guerre non linéaire*). Ainsi que le suggère cette analyse personnelle de Céline Gojon, rédactrice au Pôle études et prospectives du Centre de doctrine et d'enseignement du commandement de l'armée de Terre (CDEC)[134], l'on peine à appréhender d'un seul tenant toutes ces dimensions qui, pourtant, se prêtent difficilement à une dissection atomiste. Étudiant l'approche récente américaine du « combat multi-domaines » ou *Opérations Multi-Domaines* (MDO), le dénominateur commun aux champs immatériels, poursuit Céline Gojon, semble donc être l'*environnement informationnel*. La France reprend et consacre depuis lors l'effort doctrinal de l'armée de Terre à travers la notion d'*effets sur les champs immatériels* (ECIm*) conçus comme « *la convergence de l'environnement informationnel, du cyberespace, et l'environnement électromagnétique*.[135] » Mais, la doctrine américaine va plus loin : elle fusionne ces trois champs et intègre les effets

[133] Jean-Louis Gergorin et Léo Isaac-Dognin, *Cyber…*, *op. cit.*, p. 15.
[134] https://www.c-dec.terre.defense.gouv.fr/images/multimedia/photo/une/20220114_champs-immateriels/20211125_NP_CDEC_PEP_Champs_immateriels_un_combat_de_l-information.pdf
[135] https://www.c-dec.terre.defense.gouv.fr/images/documents/documents-doctrine/20210929_NP_CDEC_DDO_RFT_3-2-0-CEFT.pdf

des contenants (« *vecteurs et traitement de l'information* ») et des contenus (ex. : les RSN) en les unifiant tous dans la *guerre de l'information*.

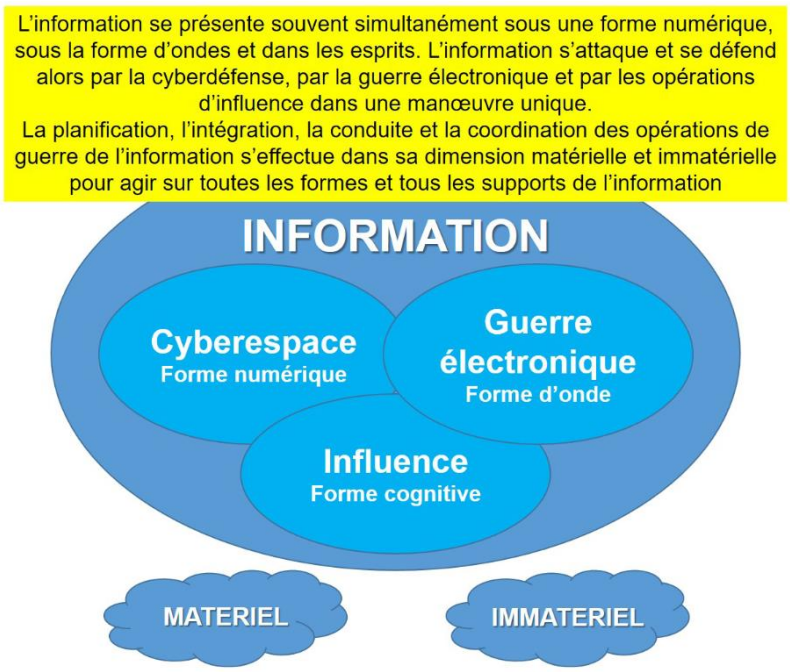



**Figure 9 :** *L'information comme dénominateur commun aux champs immatériels et matériels*

Source : Céline Gojon, *Champs immatériels, un combat de l'information*, CEDC–Pôle études et prospectives.

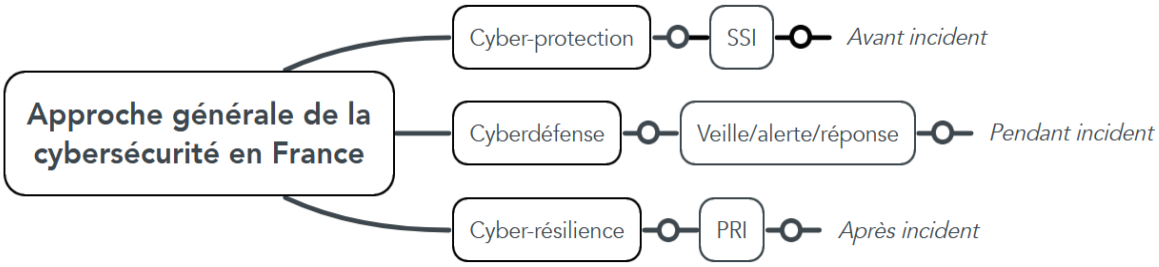
Au-delà de cet effort d'intégration, y compris au sein des Armées françaises, semble toutefois non pensée l'approche globale d'un continuum militaire-civil, public-privé. Les débuts sont pourtant venus du monde civil.

### a) *Genèse de la cybersécurité en France*

Dès 1986, la France créé une Délégation interministérielle pour la sécurité des systèmes d'information (DISSI). « *De cette époque date* [...] *une fâcheuse habitude d'additionner les organismes consacrés à cette question : des Finances à l'Intérieur, en passant par la Défense ou Matignon, chaque ministère revendique alors une part de compétence.*[136] » En 1996, le Secrétariat général à la défense nationale (SGDN) hérite de la gestion des risques informatiques puis, en son sein, la Direction centrale de la sécurité des systèmes d'information (DCSSI) en 2001. Mais chaque ministère a la charge de sécuriser ses propres SI.

[136] Nicolas Arpagian, *op. cit.*, p. 100.

En 2008, le LBSDN vient rationnaliser ces dysfonctionnements en annonçant la création d'une agence dédiée à cette coordination, c'est l'ANSSI qui voit donc le jour l'année d'après. Le LBSDN 2103 élargit la SSI des administrations publiques aux opérateurs d'importance vitale (OIV), dont les obligations en termes de conformité de sécurisation les contraignent aux audits techniques de l'ANSSI, dotée d'un pouvoir réglementaire. Entre temps, un *Pacte Défense Cyber 2014-2016* est lancé par le Ministère de la Défense en 2014 pour répondre au défi de protection des armées et des industries ; est notamment annoncée la création d'un Pôle d'excellence cyber (Rennes) et une Réserve citoyenne de cyberdéfense (RCC), promu le renseignement d'intérêt cyber (RIC) et préconisé le « *développement d'équipements et de logiciels souverains* »[137]. Puis en 2015, actualisant sa version originelle datée de 2011, l'ANSSI publie la *Stratégie nationale pour la sécurité du numérique* qui va amorcer un changement dans l'approche jusqu'ici « *technico-militaire de la cybersécurité, c'est-à-dire fondée uniquement sur la protection et la résilience des systèmes d'information et de communication*.[138] » La carte mentale ci-dessous figure la vision d'avant 2015.




*PRI : Plan de reprise informatique.*

**Figure 10 :** *Approche générale de la cybersécurité en France avant 2015*

Source : carte mentale basée sur les propos de Cédric Perrin, ancien officier cyber de la DRSD[139].

[137] https://archives.defense.gouv.fr/content/download/239576/2745135/Présentation du pacte Défense cyber.pdf. Les équipements et logiciels souverains en question n'ont jamais vu le jour ou presque. À notre connaissance (l'on peut se référer aux communications sénatoriales, par ex. grâce à https://politique.pappers.fr/recherche?q=%22logiciels%20souverains%22), on compte seulement le système d'exploitation à destination des administrations *ClipOS*, élaboré par l'ANSSI sur la base de Linux. Comme l'indique l'agence, il n'a pas trouvé son public et n'est donc plus maintenu (https://clip-os.org/). L'ANSSI ne l'a pas considéré comme « souverain », du moins depuis la publication de son code. Mais il était *open source*. Il est intéressant de noter que la Russie a bâti la souveraineté numérique de ses administrations en s'appuyant délibérément sur des logiciels libres et ouverts (voir Marie-Gabrielle Bertran, « La place des logiciels libres et open source dans les nouvelles politiques du numérique en Russie », *Hérodote*, 2020, *op. cit.*, pp. 235-252). Par ailleurs, on verra plus loin que la RCC n'a pas vraiment tenu ses promesses.

[138] Aude Géry, « La stratégie française de cyberdéfense », *Brennus 4.0. Lettre d'information du CDEC*, mars 2020 (https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299).

[139] Entretien avec Cédric Perrin, 05/10/2017 (alors en fonction). La DRSD (Direction du renseignement et de la sécurité de la Défense) est un SR du premier cercle.

Ainsi, une ouverture s'opère vers la sphère socio-économique ; ce que reflète le changement de lexique et formulation (« du numérique »). Elle porte cinq objectifs :

- Garantir la souveraineté nationale (*intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure*) ;
- Apporter une réponse forte contre les actes de cybermalveillance (*confiance numérique, vie privée, données personnelles, cybermalveillance*) ;
- Informer le grand public (*sensibilisation, formations initiales, formations continues*)
- Faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises (*environnement des entreprises du numérique, politique industrielle, export et internationalisation*) ;
- Renforcer la voix de la France à l'international (*Europe, souveraineté numérique, stabilité du cyberespace*)[140].

Enfin, le texte encourage l'implication des ministères de l'Intérieur, de la Justice et Affaires étrangères, ce qui permet sous la tutelle de l'ANSSI d'assurer une stratégie interministérielle, néanmoins obérée par des choix relevant encore de logiques de silotage, comme nous l'avons vu par exemple pour les COMCYBERs ou l'autonomie de certaines administrations. On note également que, pourtant bien identifiées, les questions liées à la souveraineté numérique ne cessent de faire débat depuis les appels à « l'introspection » auxquelles les institutions européennes et françaises sont censées se livrer sur ces sujets depuis la crise sanitaire : réindustrialisation, critique des *Géants du numérique* américains ou chinois, appel du commissaire Thierry Breton « à la fin de la naïveté de l'Europe » ou encore nécessité « de se faire respecter » des mots d'Emmanuel Macron.
Dans le sillage de cette *Stratégie nationale pour la sécurité du numérique*, une *Loi pour la République numérique* vient enfin non consacrer mais timidement autoriser les pratiques de hacking dit « éthique » en ne désignant pas nommément les hackers mais les assimilant à des « lanceurs d'alerte numérique ».

### b) *Avancées et vicissitudes des politiques de cybersécurité*

Par la suite, publiée par le Secrétariat général pour la défense et la sécurité nationale (SGDSN*), la *Revue stratégique de cyberdéfense* de 2018 – parfois appelé *Livre blanc de la cyberdéfense* – vient renforcer cette ouverture et confirmer la nécessité de sécuriser la société

[140] https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ ;
https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_dossierpresse.pdf

dans son ensemble, en dressant un panorama de la cybermenace et préconisant une rationalisation des chaines opérationnelles de cyberdéfense pour une « *nécessaire coordination* »[141] sous la houlette de l'ANSSI (protection, opérations militaires, renseignement et investigation judiciaire). À ce dernier égard, la *Revue* insiste sur le besoin de développer les capacités du système judiciaire pour qu'il soit « *en mesure de répondre à l'explosion du nombre de délits cybercriminels* ». Nous verrons plus loin que les carences dans le domaine sont criantes. Enfin, le texte conclut en outre que les enjeux économiques liés aux mesures proposées doivent « *encore être affermis et mieux cartographiés. Dans tous les cas, il est nécessaire que la France encourage et accompagne le développement industriel dans le domaine de la cyberdéfense, en entretenant une offre industrielle nationale, facilitant l'incubation de* start up *et contribuant à l'émergence européenne de leaders mondiaux. Si les enjeux sont majoritairement à cette échelle européenne, comme par exemple l'émergence d'un* cloud *de confiance, ceux liés à la souveraineté (numérique) ne doivent pas pour autant être oubliés.*[142] »

Si le constat est clair, les suites données n'ont pas toutes été concluantes. De même, à notre connaissance, les mesures de la *Revue* concernant « *l'éducation, du plus jeune âge jusqu'aux études supérieures* » n'ont connu que des prises en compte disparates, sans coordination nationale. Certains établissements y sont attachés (souvent des initiatives individuelles d'enseignants ou de directeurs) et conduisent des opérations de sensibilisation en faisant intervenir des officiers des forces de sécurité ou des consultants spécialisés, mais il n'y a aucune obligation. Les initiatives se multiplient mais sont très récentes ou peu suivies d'effets, selon notre expérience et nos contacts dans les établissements du secondaire[143]. Dans l'enseignement supérieur – où nous intervenons personnellement –, nous constatons des disparités très fortes et le fait que peu de véritables cursus dans les écoles d'informatique soient pleinement consacrés à la cybersécurité/la SSI[144]. Par ailleurs, parmi les formations initiales dans ces cursus qui proposent des enseignements dans le *pentesting* par exemple, beaucoup négligent d'autres domaines associés au *hacking* ou du moins de la cybersécurité (OSINT*, rétro-ingénierie et forensique notamment[145]). Par ailleurs, les formations d'autres secteurs que

[141] http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf
[142] *Idem*, pp. 135, 136.
[143] Citons : https://pix.fr/ ; https://www.ssi.gouv.fr/actualite/au-college-et-au-lycee-former-a-la-cybersecurite-par-le-jeu/ (date de 2023) ; https://www.ssi.gouv.fr/administration/formations/cyberedu/
[144] Bien sûr, un socle d'informatique généraliste est nécessaire, mais la SSI est souvent une spécialité de fin de cursus (master). Parfois, certains cours de *pentesting* sont optionnels ou n'ont été intégrés que depuis peu (un an ou deux à ce jour).
[145] L'OSINT est le renseignement de sources ouvertes (investigations numériques), la rétro-ingénierie informatique consiste à étudier un logiciel pour en déterminer la méthode de programmation et le fonctionnement du code. Par exemple, on étudie les logiciels malveillants (*malwares*). Enfin, l'analyse forensique consiste à « faire parler » des supports numériques, notamment dans le cadre d'enquêtes policières/judiciaires.

l'informatique, dans le supérieur en général (écoles de commerce ou de journalisme et communication, cursus « infocom » par exemple), ne proposent que très peu de cours de sensibilisation au sujet et encore moins de formation à la discipline. C'est sur la base de nos initiatives et propositions personnelles de tels contenus d'enseignement que plusieurs établissements ont pris conscience de l'intérêt d'insérer ce « plus » dans leur offre de formation[146]. En outre, comme pour la labellisation *CyberEdu* ou hors de ce type de dispositif, un effet d'aubaine peut se faire jour chez certains établissements en termes de positionnement commercial et marketing, sans que l'intérêt d'utilité publique soit réellement partagé ni même compris. À cet égard et pour revenir sur les écoles d'informatique à proprement dites, proposer des cours de *pentesting* est particulièrement intéressant mais la question se pose de savoir si ceci est pensé tel un « produit d'appel » dans les offres d'établissements privés notamment. Par ailleurs, le label *SecNumEdu*, qui permet d'assurer qu'une école d'informatique réponde aux critères de pertinence formation/objectifs définis par l'ANSSI, a fait l'objet à ce jour de trente-neuf demandes, sur au moins une centaine d'établissements spécialisés[147].

Revenons ici sur les dernières préconisations de la *Revue stratégique de cyberdéfense* de 2018 et aux enjeux de souveraineté numérique et de « cloud *de confiance* ». Dans le cadre général du projet « Andromède » impulsé sous le mandat de Nicolas Sarkozy, *CloudWatt* et *Numergy*, propositions de clouds souverains français portées d'un côté par Orange et Thales et de l'autre par SFR et Bull, ont été annulées en 2019[148]. Reste les *clouds* opérationnels de Dassault (3DS Outscale), lui plutôt projeté vers une internationalisation de son service ; OVH dont le PDG Octave Klaba a longtemps pesté (notamment sur la plateforme LinkedIn) contre les autorités françaises éludant sa proposition souveraine finalement acceptée à travers le projet *Synfonium* (dont la Caisse des dépôts est actionnaire à 25%)[149] ; enfin, le projet européen Gaia-X, porté par le « couple » franco-allemand qui semble ne pas viser les critères de véritable souveraineté et ne constituer du reste pour l'heure qu'un cadre normatif sinon une coquille vide[150]. Notons à ce sujet les difficultés françaises à appréhender ou consentir à un projet de centralisation souveraine des données de santé nationales. Ledit projet, baptisé *Health Data*

[146] Nous avons pu proposer à plusieurs établissements supérieurs d'inclure un cours, un module ou un atelier de sécurité numérique dans le cadre de leur programme. Ceci était très nouveau pour ces derniers, qui le faisaient soit en réaction à la couverture médiatique grandissante sur les cyberattaques, soit de manière plus réfléchie dans une approche de cohérence globale avec les enjeux systémiques que revêt la cybersécurité.

[147] https://www.silicon.fr/secnumedu-39-formations-labellisees-461724.html ; Le site web de l'Etudiant en dénombre au moins 99 (https://www.letudiant.fr/fiches/etudes/secteurs-informatique.html). Toutes n'ont certes pas intégré une spécialité en sécurité ; mais c'est de plus en plus rare étant donné la pénurie de profils dans le domaine sur le marché de l'emploi. Le site de l'ANSSI ne dénombre pas les écoles labellisées mais les formations : 79 à ce jour (https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/)

[148] https://www.challenges.fr/economie/le-cloud-souverain-version-sarkozy-est-mort-et-enterre_667076

[149] https://www.latribune.fr/technos-medias/internet/numerique-souverain-octave-klaba-et-la-caisse-des-depots-creent-synfonium-un-champion-europeen-qui-veut-d-emblee-croquer-qwant-958352.html

[150] https://www.lesechos.fr/idees-debats/cercle/opinion-gaia-x-un-cloud-europeen-souverain-1976239

*Hub* (HDH), sera vraisemblablement confié à l'Américain Microsoft et son cloud *Azure* et a fait l'objet de nombreuses tergiversations de la part des autorités françaises. Validé en première instance, remis ensuite en cause par la Cour de Justice européenne, puis dans son sillage par la CNIL et le Conseil d'État en 2022, le choix initial du gouvernement sous le premier mandat d'Emmanuel Macron est finalement peu ou prou confirmé, du moins jusqu'à 2025[151]. Bien entendu, la question fait polémique, car malgré les promesses de Microsoft et l'assurance technique apportée par l'ANSSI que les données de santé resteront souveraines, la puissance du lobbyisme déployé par de tels acteurs états-uniens semble insondable. Un fonctionnaire de l'ANSSI en activité et sous anonymat[152], ne dit pas autre chose. L'ANSSI avait été pressée par le gouvernement de trouver le moyen d'assurer que le minimum serait fait en termes de sécurisation du HDH. C'est donc dans le cadre de la certification de sécurité de *clouds* étrangers baptisée *SecNumCloud*, par ailleurs tout à fait louable, que s'est inscrite la reconnaissance du prestataire américain, sur la base d'une qualification passablement modifiée. En effet, le terme retenu dans ce processus de labellisation a glissé de services/prestataires « souverains » à « de confiance ». « Bob » confie : « *on met du scotch ; c'est de la rétention minimale de données.* [...] *Le gouvernement voulait que ça aille vite.* [...] *Difficile d'être souverain, et notamment parce qu'il n'y a aucune vision stratégique de la part du gouvernement, à part une vision court-termiste.* [...] *La start-up nation de Cédric O, c'est du bullshit* [sic]. *On occulte un peu trop la réalité dans la culture de la communication politique.*[153] »

Comme faisant écho à ces considérations, la *Revue stratégique de défense et de sécurité nationale* de 2017 rappelle à raison que « *les plateformes d'intermédiation privées nées de la révolution numérique, comme Google, Facebook ou Baidu* » sont des acteurs pesant lourdement dans les relations internationales. « [...] *Ces entreprises collectent et contrôlent d'immenses volumes de données et assurent désormais des services essentiels. La détention, le croisement et l'exploitation de ces informations constituent un avantage majeur dans le domaine économique, mais aussi stratégique (connaissance, anticipation, etc.)* [...] *La suprématie des États-Unis dans toutes les dimensions de l'espace numérique (matérielle, technologique, économique, juridique, politique et militaire) offre un contraste saisissant avec la situation des Européens, qui demeurent fortement dépendants de l'extérieur et dont les investissements comme les acteurs peinent à atteindre une taille critique.*[154] »

La stratégie française de cyberdéfense repose sur un principe caractéristique de séparation organisationnelle et fonctionnelle des capacités offensives et défensives souligne en

[151] https://www.silicon.fr/health-data-hub-microsoft-2025-464572.html
[152] Comme il sera précisé de nouveau plus loin, nous l'appellerons « Bob ».
[153] Entretien avec « Bob », 15/10/2021. Déjà sous pseudonyme, celui-ci a voulu être anonymisé.
[154] https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue_strategique_dsn_cle4b3beb.pdf, p. 46.

substance Aude Géry[155]. Par comparaison, de nombreux pays comme les États-Unis, le Royaume-Uni, la Corée du Sud, l'Espagne, la Turquie ou encore les Pays-Bas disposent d'un commandement unifié et, ce faisant, d'un certain degré d'autonomie[156]. Par exemple, le USCYBERCOM* américain a le même statut que ses homologues intégrés : le STRATCOM* – dont il dépendait à l'origine –, l'AFRICOM, l'EUCOM, l'INDOPACOM[157], etc. Le directeur du CYBERCOM est en même temps celui de la NSA. Or, pointe Aude Géry, « *cette séparation contient cependant des ambiguïtés*.[158] » En effet, l'ANSSI bénéficie d'un mandat pour procéder à des opérations techniques de caractérisation d'une cyberattaque subie et de neutralisation de ses effets en pénétrant les SI qui en sont à l'origine ; ce qui, *de facto*, place ces opérations techniques dans le spectre des techniques offensives. En revanche, cela peut assurer une rapide neutralisation des conséquences de ce type d'agression et donc une meilleure résilience.

Dans ce sens, l'annonce en 2018 de la publication d'éléments doctrinaux en termes de *Lutte informatique offensive* met la France en porte-à-faux et dans une certaine contradiction. Appelant à plusieurs reprises à une stabilité du cyberespace et pointant la menace que font peser certains acteurs ne souhaitant pas se rallier aux efforts de régulation internationale idoine, les autorités transmettent un message ambigu puisqu'elles assurent être en capacité d'opérer et même réaliser des cyberattaques. De surcroît, présenter l'ANSSI comme une autorité de cyberdéfense et dans le même temps de cybersécurité prête à confusion. Dans une logique très régalienne, les réponses apportées à la cybermenace *lato sensu* sont très largement de nature militaire. On voit que la répartition des rôles n'est pas encore bien définie. Cela se comprend, car il est certes ardu de traiter efficacement la complexité systémique qu'induit le cyberespace, qui se prête mal à quelque découplage particulier. D'une certaine façon, les mots de Phillipe Truillet, professeur d'informatique à l'IRIT, résonnent : « *On a trop segmenté en France entre disciplines ; et donc en informatique, robotique, IA, sciences humaines et sociales… Il n'y a pas d'interface entre elles ou alors ça vient trop tard*.[159] »

Autre ambiguïté : celle que porte la notion de *souveraineté numérique*, pourtant systématiquement mentionnée et prônée dans les différents textes. Aude Géry parle

[155] https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299
[156] Joseph Henrotin, « Cyberdéfense : une généalogie », in *La Cyberdéfense*, *op. cit.*, pp. 115-122. En 2018, la *National Cyber Strategy* permettait en outre au CYBERCOM de réaliser de son propre chef plus facilement des cyberattaques. (Voir https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf).
[157] C'est vraisemblablement cette restructuration (auparavant, ledit commandement était centré sur le pacifique et s'appelait USPACOM), qui a favorisé l'accord tripartite AUKUS (*Australia*, *United Kingdom*, *United States*), lequel a été annoncé de manière fulgurante et aux dépens de l'axe stratégique indopacifique français. En 2021, la commande de sous-marins de conception hexagonale (Naval Group) est unilatéralement annulée par le gouvernement australien, après des mois d'offensives informationnelles contre l'entreprise française.
[158] https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299
[159] Entretien avec l'auteur, 15/09/2017.

« *d'ambiguïté sémantique* » et souligne le déséquilibre manifeste posé par cette posture souveraine et les ambitions sans substance qu'elles sous-tendent en pratique. Largement popularisé et pensé stratégiquement par le fondateur de la radio *Skyrock*, Pierre Bélanger en 2010, le concept de « souveraineté numérique » a fait florès sans toutefois se matérialiser politiquement. Même si le terme n'a pas été abandonné dans les différents textes, ces derniers définissent cette souveraineté comme « *la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant parti de la numérisation croissante de la société*.[160] » Ce qui fait dire à Alix Desforges que plutôt qu'une souveraineté, il s'agit d'une « autonomie stratégique numérique »[161]. Or, il faut pour cela des technologies dont on a la maîtrise, dans les dispositifs de cryptographie[162], les systèmes de détection ou prévention d'intrusions (contre les cyberattaques) ou encore avec les services de *cloud computing*. Si l'idée explicite des textes français consiste à s'appuyer par mutualisation sur l'Europe pour assurer cette souveraineté, il faut toutefois préciser qu'en dépit des difficultés pour la seule France d'atteindre une masse critique, certaines initiatives ont pourtant démontré plus de volontarisme politique. En particulier, alors aux affaires au ministère de l'Économie et du Redressement productif, Arnaud Montebourg avait proposé en 2013 trente-quatre plans de relance industrielle dont plusieurs étaient centrés sur le numérique, avec vocation de se prémunir de l'espionnage économique : *cloud*, cybersécurité, objets connectés, etc. Étant entendu que le cyberespace amène inévitablement plus de complexité, comment être autonome stratégiquement en étant largement dépendant de technologies étrangères et en particulier états-uniennes ? En guise d'exemple, nous pensons au contexte qui a vu la création de la Direction du renseignement militaire (DRM*) en 1992. Les enseignements tirés de la première guerre du Golfe avaient montré que la France ne disposait pas d'autonomie stratégique en termes de renseignement géospatial, rendant le pays totalement dépendant des moyens techniques américains[163]. En mobilisant le savoir-faire de plusieurs sous-traitants

[160] http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf, p. 93.

[161] https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299. Alix Desforges, « Souveraineté numérique en France : du débat polarisé aux actes dispersés », in *La Cyberdéfense*, *op. cit*., pp. 127-133.

[162] On peut noter ici le savoir-faire et l'indépendance française en la matière. D'ailleurs, deux projets français ont été retenus en 2022 par le NIST américain pour préparer la cryptographie post-quantique (résistance à la cryptanalyse quantique) : les algorithmes *CRYSTALS-Kyber* (chiffrement asymétrique), et *CRYSTALS-Dilithium*, *FALCON* et *SPHINCS+* (signatures électroniques). Voir https://www.inria.fr/fr/quatre-algorithmes-certifies-NIST-menace-ordinateur-quantique.

[163] Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002, 741 p., pp. 349-350 ; Franck Bulinge, *De l'espionnage au renseignement. La France à l'âge de l'information*, Vuibert, 2012, 350 p., pp. 75-78.

comme par exemple Boostec[164], petite entreprise d'Occitanie – ô combien stratégique – mais aussi des groupes comme Thales (TAS) et surtout Astrium (ex-Airbus DS), la France avait pu bénéficier d'un satellite de reconnaissance autonome baptisé *Helios*. Si l'on revient sur ce qui nous occupe, le débat sur la souveraineté numérique est un serpent de mer auquel il convient de fixer la réflexion et matérialiser la stratégie, au risque de voir le reptile muer en un véritable *ouroboros*. En effet, dans le long sillage de ces débats, des groupes de travail parlementaires ont régulièrement été constitués à ce sujet. En 2019, le rapport d'une commission d'enquête puis, en 2021, une mission d'information près le Sénat concluaient sans détour :

> « *Pour défendre notre souveraineté numérique, il faut agir rapidement dans tous les champs où elle* [se] *trouve aujourd'hui fragilisée, contournée et concurrencée. Tel est l'objectif des principales recommandations de votre commission d'enquête.*
> *Il s'agit en effet d'un impératif absolu.* [...] *Quant aux acteurs technologiques nationaux, le soutien à leur apporter doit être une priorité, ce qui appelle un changement d'état d'esprit et de pratiques, notamment au sein de la commande publique.* [...] *En définitive, une souveraineté numérique est possible, à condition de nous donner les moyens de nos ambitions et de faire preuve de pragmatisme. Si les points d'équilibre sont souvent difficiles à trouver, entre protection des données et innovation, préférence européenne et ouverture sur le monde, ou encore numérisation et inclusion, votre rapporteur est convaincu d'une chose : l'absence, dans ce domaine, pendant de nombreuses années, de ligne directrice et de stratégie de l'Europe, a été préjudiciable et explique en partie la situation actuelle de dépendance décrite au fil des pages du présent rapport.*[165] »

Enfin, en 2021 est publié le texte portant la doctrine de *Lutte informatique d'influence* (L2I) qui, nous le pensons, si elle constitue une avancée notable, n'embrasse pas assez la globalité du domaine de la lutte informationnelle dont l'ampleur ne peut faire l'économie d'une approche intégrale civilo-militaire, publique-privée. Ce n'est du reste qu'en 2022 que l'influence sera consacrée 6e fonction stratégique par le chef de l'État, précipitée plus par le poids des circonstances et une conscience tardive de l'enjeu informationnel qui se manifeste en terrain « russo-sahélien » que par cohérence organisationnelle et réflexion stratégique. Comme le souligne à juste titre le contre-amiral (2S) Jean Dufourcq, « *l'influence ne se décrète pas, elle se construit et doit s'inscrire dans une démarche globale conforme à notre mode de gouvernance.*[166] » En outre, par nature rétive à toute logique de légitimité d'ordre juridique

[164] Mersen Boostec est une PME des Hautes-Pyrénées (Bazet) qui a un savoir-faire très rare, à savoir la fabrication de structures optiques à base de carbure de silicium, entrant notamment dans la composition des miroirs des télescopes satellitaires.

[165] Franck Montaugé (président) et Gérard Longuet (rapporteur), *Rapport de Commission d'enquête n°7 (2019-2020) "Le devoir de souveraineté"*, Sénat, déposé le 01/10/2019. (https://www.senat.fr/notice-rapport/2019/r19-007-1-notice.html) ; Jean-Luc Warsmann (président) et Philippe Latombe (rapporteur), *Rapport d'information sur le thème "Bâtir et promouvoir une souveraineté numérique nationale et européenne"*, Assemblée nationale, 29/06/2021 (https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information#).

[166] Jean Dufourcq, « L'influence comme 6e fonction stratégique », *Revue Défense Nationale*, 2023/1 (N° 856), pp. 49-52.

mais bien plus certainement idéologique, la guerre de l'information devra conduire la L2I à mener un combat à la hauteur de celui mené sans scrupules et sur tous les terrains par les ennemis ou adversaires de la France. En 2021, enfin, la *Stratégie nationale pour la cybersécurité* entend animer la sensibilisation de terrain via la gendarmerie nationale auprès des TPE/PME, puis favoriser la création de synergies, d'une part en forçant les feux sur la formation en sécurité informatique en vue de combler les besoins en ressources humaines sur le marché de l'emploi ; d'autre part en annonçant l'imminence de la livraison du Campus Cyber présenté comme le « lieu-totem de la cybersécurité française », avec pour vocation de développer le partage et les collaborations entre tous les acteurs de l'écosystème numérique.

À cet égard, les avis sur cette initiative sont partagés. Certains acteurs voient dans le Campus Cyber un simple « *projet immobilier, pour l'heure* » et « *beaucoup de com'* », comme le hacker franco-sénégalais Clément Domingo, se posant la question des liens avec les hackers indépendants, non issus du sérail[167]. Julien Métayer, hacker et OSINTer de son état, précise quant à lui : « *Je ne suis pas sûr que ça fonctionnera bien, à cause des liens contractuels liant chaque acteur avec ses propres clients.*[168] », préconisant plutôt la décentralisation. À l'heure actuelle, un Campus Cyber régional a été inauguré en Nouvelle-Aquitaine[169]. Tandis que la Professeure Frédérick Douzet, sans connaître les lieux, estime que grâce à l'ANSSI, le Campus constitue une ouverture vers le monde académique[170] et la sphère privée, tout en nourrissant la formation en cybersécurité dans le pays. Cela fait sens à son avis et en théorie et peut favoriser les collaborations du fait de la proximité des différents acteurs. Pour leur part, Victor Poucheret et Brice Augras saluent un projet intéressant : « *c'est une bonne démarche* [...] *si ça peut rapprocher les entreprises, parce que chacun a son savoir-faire* [...] *c'est tellement transverse* [...] *il faut arriver à trouver un modèle complémentaire.*[171] » De son côté, Karim Lamouri, entrepreneur et cofondateur de Hackers Without Borders, relativise : « *C'est un bâtiment. Ça canalise un temps les forces vives. C'est un projet immobilier. Ce n'est pas essentiel.*[172] » Enfin, Pierre Penalba, ex-policier spécialisé dans la lutte contre la cybercriminalité, évalue et fustige :

> « *Le Campus Cyber ? Probablement un minimum de synergie, avec un peu de compétence, mais globalement surtout une opération de communication et immobilière. C'est dommage qu'on ne sache pas travailler avec des cyberhackers français ! C'est ce qu'essaie de proposer Hackers Without Borders. Ça va prendre du temps. Le pouvoir est trop centralisé en France. Pourquoi ce projet de campus à Paris?*

[167] Entretien avec l'auteur, 15/11/2021.
[168] Entretien avec l'auteur, 30/03/2022.
[169] https://campuscyber.fr/ ; https://www.campuscyber-na.fr/
[170] Reste à savoir lequel, ce monde étant lui aussi très cloisonné et dans des postures de rivalité flagrantes. Entretien avec l'autrice, 30/03/2022.
[171] Interview de Brice « Zax » Augras et Victor « Doomer » Poucheret, chaine *Thinkerview*, 24/09/2021.
[172] Entretien avec l'auteur, 07/07/2023.

> *Et puis, on travaille au campus avec des entreprises, mais le comble c'est qu'il y a beaucoup de boîtes américaines qui n'ont rien à faire là ! Il y a des "promoteurs" venant des USA et qui infiltrent toute la communication autour du campus cyber et vendent des solutions américaines. Ils ont les compétences, mais ils n'ont rien à faire là !* [173] »

Pour résumer, les politiques de sécurité numérique ont en France fait l'objet d'un soin particulier. En 2018, Alix Desforges concluait sa thèse en disant qu'en dépit de ces efforts louables, hésitations, atermoiements et limites caractérisaient les processus décisionnels – eux-mêmes opaques et aléatoires – et que la sécurité nationale dans le cyberespace était encore perfectible[174]. De plus, en prenant des mesures actives de protection en termes de cybersécurité, les États dont la France faisaient paradoxalement augmenter le niveau de cybermenace et de tensions internationales et intranationales. La *sécuritisation* dont on a parlé *supra* est effectivement un pari risqué, celui de confondre comme le souligne Rayna Stamboliyska le sentiment de sécurité avec la réalité de cet état. À tout prendre, si communiquer sur le fait que l'on se protège et qu'on attaque accroît la menace, alors pourquoi ne pas assumer sans ambages une posture offensive résolue ? Entre « *gadgétisation* » de l'innovation à tout prix de l'industrie du secteur, et « *gesticulations sécuritaires* » des États démocratiques[175], il est nécessaire de changer notre grille de lecture régalienne et centralisée à travers le seul prisme militaire du risque cyber. Eu égard aux « effets de manche communicationnels » du pouvoir politique pointés du doigt par nombre de spécialistes à propos du Campus Cyber ou de certaines dispositions législatives, il est somme toute légitime de conserver un esprit critique. Parmi les spécialistes en question, plusieurs *hackers* maintiennent cet esprit et sont forces de propositions. Qu'en est-il donc de ce type de profil si particulier par rapport à l'écosystème de cybersécurité nationale ?

### **2)** Parties prenantes de la sécurité numérique, acteurs du cyberespace : quelle place pour les hackers ?

« *Il nous faut des hackers !* » clamait dans les années 2010 Éric Filiol, maître-cryptologue, hacker et ancien officier de la DGSE. En 2012, sous l'influence manifeste de ce dernier, le rapport dit Bockel porte des ambitions assez inédites à l'époque en matière de souveraineté numérique, en décrivant par ailleurs de manière assez pointue la notion de hacking et appelant même à faire appel à des « *pirates informatiques* white hats » (sic). S'appuyant sur l'analyse d'Éric Filiol, le texte qu'on peut considérer comme le plus précis sur

[173] Entretien avec l'auteur, 07/07/2023.
[174] Alix Desforges, *Approche géopolitique du cyberespace : les enjeux pour la défense et la sécurité nationale : l'exemple de la France*, thèse de doctorat en géopolitique, université Paris 8, 2018.
[175] Rayna Stamboliyska, *op. cit.*, pp. 397-399.

le sujet encore aujourd'hui indique qu'il « *conviendrait de renforcer les liens avec la "communauté de hackers" présente* [...] *estimée en France à environ 4 000 personnes. Nombre d'entre eux seraient désireux de mettre leurs compétences et leurs talents au service de notre pays. Aux États-Unis, les "communautés de hackers" sont d'ailleurs largement reconnues et entretiennent des relations étroites avec les autorités chargées de la sécurité des systèmes d'information. On peut ainsi mentionner la communauté de hackers "Defcon", qui compte plus de 12 000 membres* [...] *et entretient des relations avec le département de la défense et l'Agence de sécurité nationale (NSA).*[176] »

Le constat est clair : selon Éric Filiol, « *il existe une véritable fracture en France entre un monde d'anciens qui administrent mais qui ne comprennent rien à la technique et de jeunes hackers qui maîtrisent mais qui n'administrent pas.*[177] » Pourtant, le rapport n'aura que peu d'effets concrets et nous rappelle que si les choses ont certes évolué, les propos de l'ex-officier de la DGSE restent encore d'actualité :

> « *En France, nous avons le secret pour faire de grandes déclarations et ne rien faire par la suite. On continue à faire de la théorie pendant que les hackers font de l'opérationnel. L'une des raisons de notre retard est notre incapacité à capitaliser sur une énorme ressource que nous avons : nos hackers. Il y a, à la Nuit du Hack et à Hack in Paris, une communauté de jeunes brillants que le système éducatif a complètement oubliés et délaissés. Il faut une refonte en profondeur de ce système. La force de l'Allemagne ou de l'Angleterre est de savoir aussi bien réintégrer dans un cursus de formations une personne de 20 ans que de 40 ans. En France, l'important n'est pas ce que vous êtes capable de faire mais ce que vous avez fait entre 20 et 24 ans et si vous n'êtes pas normalien ou polytechnicien, vous n'avez pas droit de cité.*[178] »

Aujourd'hui, la *Nuit du Hack* est devenue *Le Hack* et les services de renseignement, de sécurité et l'armée viennent observer, approcher et parfois recruter ces profils atypiques. Mais dans quelle perspective et surtout, par quelle articulation avec le monde politique et au service de quelle stratégie nationale ?

Le hacker est-il toujours *hostis humani generis*, pirate « ennemi du genre humain » ? Si l'on considère la production doctrinale et législative précitée, le mot hacker n'apparaît presque jamais et, le cas échéant toujours pour désigner le *pirate informatique* agissant pour le compte d'une puissance étrangère. Il faut dire que des précédents ont grevé l'image du hacker, les faisant passer pour des « barbouzes numériques » durant de nombreuses années. L'affaire

[176] Jean-Marie Bockel (sénateur), *Rapport d'information au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Sénat, 18/07/2012 (https://www.senat.fr/rap/r11-681/r11-6811.pdf).
[177] *Idem*, p. 109.
[178] https://www.itpro.fr/eric-filiol-france-incapable-capitaliser-hackers-20026/

désormais bien connue du piratage de Yannick Jadot par EDF est éclairante à cet égard[179]. Et les rapports entre l'État et les *communautés* de hackers ont en France très mal commencé, comme nous le verrons plus loin avec l'opération montée par la Direction de la surveillance du territoire (DST*). Ces exemples notables sont significatifs de la perception erronée qui a longtemps prévalu autour de la figure du hacker dans notre pays. Penser néanmoins que cette vision serait aujourd'hui dépassée est idéaliste. Ainsi, aucun texte officiel cité ne reprend l'idée pourtant ancienne du rapport Bockel de faire concrètement appel à des hackers. Par exemple, interrogée à ce sujet, Frédérick Douzet dit de la *Revue stratégique de défense et de sécurité nationale* de *2017* qu'elle ne formule pas de préconisations sur l'emploi ou la contribution de telles forces vives[180].

Comme le mentionnait déjà le rapport Bockel, l'on compte de nombreux hackers souhaitant apporter leur concours y compris gracieux dans une perspective d'utilité publique. Toutefois, derrière les discours récents affichés du politique, plusieurs ombres viennent noircir le tableau. L'anecdote de deux hackers français est intéressante à ce propos. Victor « Doomer » Poucheret et Brice « Zax » Augras, deux jeunes hackers bretons, évoquent leur expérience quant à leur désir de servir la Réserve citoyenne de cyberdéfense (RCC). **En aparté, la RCC est largement qualifiée « d'usine à gaz » par les experts confirmés de la cybersécurité[181]. Beaucoup de gens non qualifiés ou pas spécialement concernés sont venus grossir ses rangs, entrainant une congestion qui a contribué à la banaliser et en atténuer l'utilité réelle sur le terrain**. Ce qui nous ramène finalement au côté tendanciel, à l'effet de mode presque inhérent aux TIC et donc à tout ce qui est « cyber », effet auquel – nous l'avons dit – peut être réceptive une part de la classe politique mais pour de mauvaises raisons. À ce propos, Éric Filiol ironisait : « *on est dans le "*bling bling*" de l'informatique : on a dans l'informatique ce qu'on a dans la politique. Il faut des menus déroulants partout, des interfaces flashys, mais dès qu'on parle de sécurité on est pris pour des emmerdeurs de première.*[182] » En ce début de décennie 2020, cela a-t-il réellement changé ? Revenons à nos deux hackers : Victor Poucheret et Brice Augras souhaitent donc

[179] https://www.lesechos.fr/2011/11/affaire-greenpeace-edf-condamnee-pour-espionnage-413005. En 2006, alors directeur de Greenpeace, Yannick Jadot est victime d'un piratage commandité par EDF qui cherchait à contrecarrer les campagnes anti-nucléaires de l'ONG.

[180] Entretien avec l'autrice, 30/03/2022. Elle a supervisé son élaboration.

[181] Pour en faire personnellement partie, nous confirmons cette perception en appui avec les témoignages issus de nos entretiens. C'est par le biais – légitime et cohérent – de la Réserve de la gendarmerie que cela nous a été permis, mais cette voie n'est pas généralisée dans le pays. Il n'y a guère de coordination nationale au niveau de la RCC, et de notre côté des acteurs ont organisé indépendamment une RCCO(ccitanie) basée à Toulouse (elle compte une dizaine de personnes).

[182] https://www.lemonde.fr/blog/bugbrother/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/. Éric Filiol renchérit : « *On parle beaucoup de réserve citoyenne, mais si c'est pour le faire uniquement avec des polytechniciens, des normaliens et des centraliens, on va pas aller très loin*. » (Interview *Thinkerview* du 02/07/2013, https://www.youtube.com/watch?v=Fn_dcljvPuY).

intégrer la Réserve en 2020 dans le cadre du FIC auprès du stand de l'Armée. « *On a posé la question, mais ça ne s'est pas bien fini*. » souligne Brice Augras. Ces derniers déplorent avoir été pressentis pour devenir de simples « *ambassadeurs* » qui « *plairaient aux jeunes* » dans le cadre de sensibilisations[183]. Finalement, un casting mal appréhendé compte tenu du fait que le CV demandé aux deux experts par l'Armée à cette occasion ne peut rendre honneur au niveau technique dont les deux hackers sont auréolés par leurs pairs. La question se pose : des talents sont-ils gâchés ? D'autant que les bonnes volontés ne manquent pas. Brice Augras évoque dans ce sens son activité *pro bono* avant la création de son entreprise. Ce dernier allait visiter des pharmacies qu'il avait *pentestées* pour les alerter quant aux failles que leur prestataire informatique avait laissées, bien souvent nonchalamment. Et de citer en dernier exemple l'idée d'un engagement inconditionnel en cas de mobilisation militaire, pour mettre à disposition leurs compétences techniques dans la sécurité informatique du pays.

Par ailleurs, dans un contexte de pénurie d'experts en cybersécurité, certaines tensions sont apparues concernant la politique de recrutement de l'ANSSI, laquelle fait l'objet de vives critiques, même si l'on comprend aisément l'enjeu de disposer des meilleures chances. En l'occurrence, plusieurs spécialistes évoquent la tendance de l'agence à phagocyter le marché des informaticiens en cybersécurité. Le journaliste d'investigation spécialiste du numérique Jean-Marc Manach évoque même un « siphonnage » et est rejoint dans cette optique par Jean-Nicolas Piotrowski, Clément Domingo ou encore Damien Cazenave pour qui, l'ANSSI « *assèche le marché des ressources humaines en sécurité informatique*.[184] » Malgré ces frictions somme toute compréhensibles, l'ANSSI ne pouvant rivaliser avec les rémunérations pratiquées dans les entreprises, le phénomène dénote toutefois un manque de coordination et une mise en concurrence dommageable entre acteurs publics et privés. En outre, le mandat de Guillaume Poupard a été unanimement salué par la communauté des hackers français auprès de laquelle il a fait opérer à l'ANSSI un rapprochement inédit. De son propre aveu, ce dernier souligne les avancées réalisées mais regrette toutefois avoir eu encore à butter contre des « murs » administratifs[185].

Les autorités étatiques initient cependant des démarches intéressantes pour faire appel à la communauté des hackers à travers les programmes de *bug bounty*. Et la *Loi pour la République numérique* de 2016 apporte enfin un cadre juridique aux activités de hacking éthique, sans toutefois aller assez loin. C'est dans ce sens que la sénatrice Natalie Delattre a proposé, fin juin 2023, un projet d'amendement à cette disposition dans le cadre de la Loi de

[183] Interview de Brice Augras et Victor Poucheret, chaine *Thinkerview*, *op. cit*. Ils ont fondé une entreprise spécialisée dans les audits de *pentesting*, BZHunt.
[184] Entretiens avec « Bob » (15/10/2021), Damien Cazenave (24/07/2017), Jean-Marc Manach (14/04/2023) et Jean-Nicolas Piotrowski (30/07/2017).
[185] Entretien avec l'auteur, 17/04/2023.

programmation militaire 2024-2030. Ce dernier porte sur la reconnaissance officielle du statut de *hacker éthique* en droit français et de fait leur protection comme « lanceurs d'alerte numérique »[186]. Cela constitue une avancée indéniable mais atteste aussi de cette difficulté perpétuelle à poser les termes du sujet, le prendre à bras-le-corps, comme s'il s'agissait d'une activité peu avouable, encore une fois de manière analogue avec le renseignement. La seule impossibilité d'assumer en France l'expression *intelligence économique* est révélatrice[187]. « Lanceurs d'alerte numérique » ? Hackers « éthiques » : hackers *légaux* en réalité. « Hackers-corsaires » ? Hackers au service de leur État préférablement. Contacté dans le cadre de notre travail, Bernard Barbier, ancien directeur technique de la DGSE, ne souhaite pas communiquer. Ce n'est pas parce qu'on ne le sait pas que les services de renseignement ne communiquent pas avec les hackers et n'entretiennent pas des liens avec eux, dit-il en substance. Qu'y a-t-il donc de secret ? Surtout : communiquer est-ce bâtir ensemble ?

Les hackers sont probablement le type d'acteurs le mieux placé dans l'écosystème de la cybersécurité nationale. Au carrefour de l'innovation informatique et des pratiques de savoir-faire technique, ils cherchent/trouvent des failles, explorent et réinventent des architectures logicielles, contournent des sécurités pour les rendre plus efficientes… En un mot, celui de Barnaby Jack[188], « *Parfois, il faut démontrer l'existence d'une menace pour susciter une solution*. » Mais sont-ils sollicités à leur juste mesure, à hauteur de leur capacité à contribuer à la cybersécurité du pays ? Comme le souligne Victor Poucheret :

> « *Les meilleurs spécialistes sont d'esprit indépendant. La position du hacker en général, c'est un peu l'image de l'électron libre. Et il faut un esprit d'attaquant, et dans l'actualisation perpétuelle des connaissances qu'il s'agisse des outils, des progrès de la technologie et de la cybermenace.* […] *Il y a la question des valeurs de la France dont le pays en général fait grand cas. C'est ce qui fait partie de notre identité nationale. Et ça entrave peut-être notre progression en termes de cybersécurité.*[189] »

Tentons donc d'en savoir un peu plus sur ces « électrons libres », dont l'image souffre encore de bon nombre de préjugés, fussent-ils négatifs ou positifs.

[186] https://www.senat.fr/seances/s202306/s20230628/s20230628008.html ; https://videos.senat.fr/video.4011095_649c1f7021980?timecode=10424340

[187] Le rebaptême de la Délégation interministérielle à l'intelligence économique(D2IE) en Service d'information stratégique et de sécurité économique (SISSE) est révélatrice.

[188] Barnaby Jack (2013†) était un hacker néo-zélandais. Il a démontré par la preuve (de concept – PoC) qu'il était possible de pirater des guichets automatiques, et surtout des pacemakers et pompes à insuline d'hôpitaux.

[189] Entretien avec l'auteur, 14/11/2021.

# Chapitre 2 | La figure du hacker, entre idéalisation et incompréhension

« *Le hacker a trois traits de caractère :*
*Anticonformiste, engagé et créatif.* »

Ted Harrington

À l'instar des officiers de renseignement, les hackers sont l'objet de nombreux stéréotypes qui alimentent une fantasmagorie entre crainte et fascination. Pourtant, « *le hacking, c'est une démarche scientifique* » avance Jérémie Zimmermann, ancien porte-parole de l'association La Quadrature du Net[190]. C'est avant tout un état d'esprit, une culture voire une philosophie de vie qui s'incarnent dans les valeurs de partage, de liberté et d'excellence. Au regard des préceptes des arts martiaux chinois, on pourrait d'ailleurs dire que les hackers cultivent le *kung-fu*[191] de l'informatique et des technologies qui y sont liées. **Le hacking n'est pas en soi un délit, c'est l'art de comprendre les mécanismes sous-tendant un système pour en contourner le fonctionnement normal**. Dans nos sociétés très policées où tout est appréhendé à l'aune du risque, ce type d'approche peut sembler incongru voire facteur de subversion. Il est vrai que le principe même de cette philosophie tourne autour d'une logique de transgression. Les communautés de hackers sont d'ailleurs fondées sur des activités partagées à la charge fortement symbolique. À rebours des poncifs, le hacker n'est pas un *geek* asocial et isolé sans son coin. Bien qu'ils travaillent souvent individuellement, les hackers tissent ainsi des liens sociaux denses avec leurs pairs dans une optique d'émulation, avec pour horizon l'amélioration collective et le partage communautaire.

Bien sûr, cela n'empêche pas la compétition et malgré une positivité générale, des tensions peuvent être observées, d'autant que plus qu'un groupe homogène, les hackers forment des communautés parfois disparates, mais dont la culture cyber et informatique est le fondement collectif. Entre spécialistes de la SSI, experts dans la sécurité des dispositifs physiques, rétro-ingénieurs du code, *pentesters* ou *redteamers*, et hackers à proprement parler, l'état d'esprit propre à chacun n'est pas tout à fait le même voire entre en opposition avec celui des autres. Deux principales approches se complètent en se confrontant, souvent pour le meilleur : la position des défenseurs et la posture des attaquants, souvent résumées

[190] Sylvain Bergère, *Une contre-histoire de l'internet*, film documentaire, *Premières lignes Télévision*, 2013, 86mn.
[191] En chinois (mandarin *Gōngfū*), le terme signifie littéralement le « mari du travail » et plus largement « l'accomplissement individuel » dans quelque activité au prix d'efforts acharnés ; l'excellence vers laquelle on tend, avec patience, opiniâtreté et stratégie ; l'habileté et la discipline dans l'acquisition de compétences. Loin du stéréotype des films d'arts martiaux venus de Hong-Kong et véhiculé par le cinéma hollywoodien des années 1970.

dans les concepts conjoints de *blue team* et *red team*. Au-delà de cette partition binaire convenue, l'essence du hacker repose peut-être, en interface, sur la figure de l'*hacktiviste*. Car les hackers actuels, sans renier l'héritage des illustres pionniers, ont toutefois un peu changé.

## A. *Hackers : mythes et réalités*

*« Oui, je suis un criminel. Mon crime est celui de la curiosité.*
*Mon crime est celui de juger les gens selon ce qu'ils pensent et disent, pas selon leur apparence.*
*Mon crime est d'être plus malin que vous, quelque chose que vous ne me pardonnerez jamais.*
*Je suis un hacker, et ceci est mon manifeste.* »

Loyd « The Mentor » Blankenship

En 1995 sort le film *Hackers* de Iain Softley avec Angélina Jolie dans le rôle d'« Acid Burn », qui inspirera sa vocation à Keren Elazari, une hackeuse israélienne[192]. Avec des fortunes diverses, quelques autres productions de fiction viendront bâtir l'imagerie d'Épinal de la figure du hacker, jusqu'à la série *Mr Robot* lancée en 2015. Celle-ci concentre tous les aspects du phénomène, mêlant la mythologie originelle d'un mouvement utopiste et profondément politique, avec les aspects fascinants du savoir-faire technique de ces héros du code. Si le propos est confus, l'histoire décousue et le message ambigu, ce rejeton du capitalisme hollywoodien absorbé, digéré et propulsé tel un produit vantant paradoxalement l'anarchisme et l'anticapitalisme est encensé par la critique. Pour une fois, du reste, les techniques de piratage utilisées sont plausibles voire crédibles : intrusions dans des systèmes, emploi d'outils existants, bouts de code réel filmés à l'écran, usage de l'ingénierie sociale… la série rend enfin – un peu – justice aux hackers. Est-ce symptomatique de l'époque ?

De *La conscience du hacker* de Loyd Blankenship aux *manifestes cypherpunk* en passant par celui de la sociologue américaine McKenzie Wark, *L'éthique des hackers* de Steven Levy ou *Le code fait loi* de Lawrence Lessig, les hackers ont leurs « textes sacrés »[193]. À leur image comme à celle de *Mr Robot* cependant, l'on comprend que le mouvement des hackers revêt les habits d'une véritable philosophie politique. Entre légalité, a-légalité et illégalité, les hackers sont difficiles à catégoriser pour ne pas dire étiqueter, ce qui constitue une première difficulté pour une société y compris démocratique promouvant la différence mais veillant au conformisme. Avant les années 1980, le mot « hacker » avait une connotation positive, c'était un « *compliment, une récompense après un travail bien accompli. Il voulait dire quelque chose comme un bricoleur ingénieux, un expert de science et de technique*. […] *Parfois, pour inventer des nouvelles choses, il faut savoir sortir des sentiers battus, explorer de nouvelles pistes. Tous les moyens sont bons !* [194] » Puis, il a perdu de son aura au gré des politiques

[192] Iain Softley, *Hackers*, film cinématographique, United Artists, États-Unis, 1995, 107mn.
[193] http://phrack.org/issues/7/3.html#article ; https://www.activism.net/cypherpunk/crypto-anarchy.html (Tim May) et https://www.activism.net/cypherpunk/manifesto.html (Eric Hugues) ; McKenzie Wark, *op. cit.* ; https://www.harvardmagazine.com/2000/01/code-is-law-html ; Steven Levy, *L'Éthique des hackers*, *op. cit.*
[194] Samuel Verley & Élodie Perrotin, *Qui sont les hackers ?*, *op. cit.*, p. 14.

sécuritaires qui en ont fait le synonyme de l'ennemi numérique numéro un. En effet, « *Les hackers nous fascinent parce qu'ils se rendent maîtres de cette technologie que nous utilisons aveuglément. Et comme nous ne comprenons pas leurs techniques, nous craignons qu'ils les utilisent à mauvais escient. Les hackers nous apparaissent comme des magiciens de l'informatique, dont nous sommes incapables de connaître les trucs ! Alors, magie blanche ou magie noire ?* [195] », Hackers *blancs* ou hackers *noirs*, à moins que le *gris* ne vienne flouter l'image d'un monde pourtant déjà instable ?

### **1)** Un état d'esprit, un savoir-faire

Les fondements mythologiques et historiques du mouvement hacker sont bien connus. Tout commence au *Tech Model Railroad Club* (TMRC) du Massachusetts Intitute of Technology (MIT) de Boston, un club de modélisme ferroviaire scindée en deux équipes. L'une chargée des trains, l'autre des circuits électriques les propulsant. Ce sont les étudiants de cette deuxième équipe qui vont populariser les mots *hack* et *hacker* pour en faire un concept du jargon des informaticiens au moment où les premiers (macro)ordinateurs électroniques font leur apparition[196]. Ils s'intéressent alors à l'IBM 704 équipant l'Institut puis au TX-0 dont le prix s'élève alors à 3M$. En 1959, le mot hacker se démocratise et définit une personne qui utilise son ingéniosité pour créer un nouveau résultat – un *hack* –, en particulier modifier un système pour l'améliorer et le rendre plus efficient. Le tout dans la logique du RTFM (*Read the F*cking Manual*), inclination à la « débrouille » qui distingue les hackers des utilisateurs lambda ne cherchant pas à comprendre le fonctionnement d'une machine. Voici la définition officielle du TMRC : « *Hacker : Une personne qui aime explorer en détail des systèmes programmables et étendre leurs capacités, contrairement à la plupart des utilisateurs, qui préfèrent n'apprendre que le minimum nécessaire.*[197] » Définition qui sera complétée par la RFC1392, le glossaire des utilisateurs de l'Internet : « *Une personne qui aime avoir une compréhension intime du fonctionnement interne d'un système, des ordinateurs et des réseaux informatiques en particulier.*[198] »

Véritable credo, le hacking va être codifié dans un livre qui fait toujours autorité. Son auteur, Steven Levy, est un journaliste spécialisé dans l'informatique, rédacteur en chef de

[195] Samuel Verley & Élodie Perrotin, *op. cit.*, p. 13.
[196] http://tmrc.mit.edu/hackers-ref.html
[197] http://catb.org/~esr/jargon/html/H/hacker.html
[198] https://www.ietf.org/rfc/rfc1392.txt. Les RFC (*requests for comments*) sont des documents décrivant des standards et spécifications techniques pour le fonctionnement de l'internet, produits par l'organisme IETF (*Internet Engineering Task Force*), un des acteurs de la *gouvernance de l'internet* (https://www.ietf.org/standards/rfcs/).

*Wired* et contributeur chez *Medium*[199]. En 1984, il synthétise leur état d'esprit dans son *Éthique des hackers*. Cette éthique est fondée sur six principes :

1. L'accès aux ordinateurs – et à tout ce qui pourrait vous apprendre quelque chose sur le fonctionnement du monde – devrait être illimité et total. Toujours se ranger à l'impératif pratique !
2. L'information doit être libre et gratuite.
3. Se méfier de l'autorité – Promouvoir la décentralisation.
4. Les hackers doivent être jugés sur leurs capacités en hacking – seule la compétence compte – et non sur de faux critères tels que le diplôme, l'âge, l'origine ou le poste[200].
5. On peut créer de l'art et de la beauté sur un ordinateur.
6. Les ordinateurs peuvent améliorer notre vie[201].

Au cœur de ce code, l'idée d'un libre accès à l'information est centrale, lequel doit pouvoir assurer le renouvellement des connaissances. Ainsi, la censure ou la rétention de l'information est rejetée et toute organisation doit être fondée sur un système ouvert et transparent dont tout le monde peut vérifier le fonctionnement, le diagnostiquer, le corriger et l'améliorer. Considérés comme des artistes voire des artisans, les hackers valorisent l'économie des moyens (par exemple en mémoire électronique) et l'élégante (entendre « efficace ») programmation d'un code source logiciel. L'ouvrage de Steven Levy décrit quatre âges de hackers : les pionniers comme Richard Greenblatt (créateur de l'ordinateur *Lisp* et des logiciels de jeux d'échecs), Steve Wozniak (cofondateur de Apple), Bill Gates (cofondateur de Microsoft), Marvin Minsky (scientifique et philosophe spécialiste d'IA), Richard Stallman (fondateur du projet GNU) ou encore John « Captain Crunch » Draper, le célèbre pirate des lignes téléphoniques Bell, connu pour avoir su détourner à cette fin l'usage d'un sifflet offert dans les boites d'une marque de céréales (Quaker Oats)[202]. La seconde génération, incarnée par Steve Wozniak, est celle des hackers *hardware*, « bidouilleurs » et concepteurs ou utilisateurs d'ordinateurs personnels (PC) comme le SOL ou l'Altair 8800 de la société MITS.

[199] *Medium* (https://medium.com/) est une plateforme de blogging. *Wired* (https://www.wired.com/) est un magazine mensuel très connu des technophiles et doté d'une coloration médiologique dans la veine du journal français *Usbek & Rica*. Herbert M. McLuhan est présenté en filigrane comme le saint-patron de *Wired*. Le magazine compte plusieurs versions nationales notamment en Europe, sauf en France où Conde Nast, sa maison d'édition, n'a pas jugé rentable son lectorat.

[200] Rayna Stamboliyska, *op. cit.*, p. 166, parle de « *"do*-ocratie*", soit le pouvoir par ceux qui font, chez Anonymous par exemple.* »

[201] Steven Levy, *op. cit.* Voir les commentaires éclairés de l'économiste Michel Volle, spécialisé en informatique (https://archive.wikiwix.com/cache/index2.php?url=http://www.volle.com/lectures/citations/hackersethic.htm)

[202] John Draper est considéré comme l'un des premiers *phreakers* dont l'activité (*phreaking*) consistait à détourner frauduleusement les systèmes téléphoniques dans les années 1960.

De cette époque datent les premières divisions intestines entre, d'un côté, les hackers-entrepreneurs et, de l'autre, les hackers-technophiles. En effet, Microsoft va être l'un des premiers à rompre le pacte implicite de la gratuité en proposant un interpréteur baptisé *Altair BASIC*[203], dont le code (sous licence) va être rapidement dupliqué sans le consentement de Bill Gates. Ce dernier écrira d'ailleurs une lettre ouverte pour dénoncer la copie logicielle, prônant une juste rémunération à ceux qui améliorent et recréent de tels programmes et *in fine* jetant les bases de la propriété intellectuelle pour les logiciels[204]. D'une certaine manière, le fameux opuscule *Code Is Law* de Lawrence Lessig constitue l'aboutissement de cette rupture consommée entre pionniers de l'informatique. En 2000, le juriste et professeur de droit avançait que *le code faisait loi* dans le sens où c'est par l'apparente neutralité de prises de dispositions techniques sur le cyberespace que les libertés fondamentales seraient menacées. Autrement dit, le code régule (droit) et gouverne (politique), et la nature originelle distribuée de l'Internet s'est rapidement confrontée aux logiques d'appropriation monopolistiques et principes de propriété intellectuelle, concourant à la remise en cause de la *neutralité du Net*[205]. On peut observer ici les profondes contradictions du système américain, généralisables dans le capitalisme libéral. Paradoxalement, un Bill Gates est rarement présenté comme un hacker. En suivant des intérêts mercantiles, il a néanmoins « hacké » un marché, dans une logique entrepreneuriale qui aux EUA fait la part belle à celui qui parvient à *disrupter* un marché ou un secteur économique. Cette culture d'entreprise de l'innovation de rupture a été sacralisée dans le pays, faisant de ces entrepreneurs « de génie » des outsiders héroïques[206]. La Silicon Valley est le fruit parfait de cette culture du contournement des règles établies propulsant de minuscules *start-up* en méga-corporations capables de changer le monde. La mythologie des garages ayant vu éclore ces jeunes TPE est révélatrice à cet égard : Hewlett-Packard, née en 1939 dans la maison personnelle de David Packard avec William Hewlett à Palo Alto ; Apple en 1976, dans l'ancienne demeure de Steve Jobs accompagné de son acolyte Steve Wozniak à Los Altos ; ou encore Google, fondée dans un garage loué par Larry Page et Sergey Brin à Menlo Park en 1998. « […] *la communauté des entrepreneurs diffère de manière significative des hackers dans son approche de l'innovation technologique. Tandis que les entrepreneurs*

[203] BASIC (*Beginner's All-purpose Symbolic Instruction Code*) est un ensemble de langages informatiques de haut niveau qui simplifie la programmation. Un interpréteur est un outil exécutant les programmes écrits dans un langage informatique.

[204] https://www.digibarn.com/collections/newsletters/homebrew/V2_01/homebrew_V2_01_p2.jpg

[205] Voir à ce propos l'intéressante analyse du juriste et bibliothécaire Lionel Maurel, qui parle même d'une inversion du *Code Is Law* en « Law is Code » (https://scinfolex.com/2014/01/24/comment-code-is-law-sest-renverse-en-law-is-code/). Lawrence Lessig est cofondateur des licences Creative Commons et a été l'ami et mentor d'Aaron Swartz.

[206] Rodrigo Nieto Gómez, « Cybergéopolitique : de l'utilité des cybermenaces », *Hérodote*, 2014, *op. cit.*, pp. 98-122.

*"piratent" les marchés à l'aide de la technologie à des fins commerciales, les hackers relèvent des défis technologiques pour le plaisir de résoudre un problème.*[207] »

Le troisième temps des hackers est, pour Steven Levy, celui des hackers-gamers, où l'esprit entrepreneurial va finalement se fondre dans l'éthique hacker. C'est l'ère des débuts des jeux-vidéo et la naissance en 1979 de la première société éditrice de *gaming softwares*, Sierra On-Line. L'un des premiers jeux-vidéo, *Spacewar!*, avait été créé en 1962 puis plusieurs fois amélioré au sein du MIT/TMRC pour tester et exploiter les capacités du micro-ordinateur PDP-1. Les marques comme Atari vont symboliser à la fois le jeu-vidéo comme défi de programmation informatique et la fin des idéaux du logiciel libre portés par les pionniers du MIT. Les premières protections anti-piratage apparaissent à ce moment-là et certains hackers sont employés par les éditeurs pour précisément trouver des mécanismes empêchant la copie. Le challenge pour les hackers est trop tentant, qui met en œuvre ce qui s'apparente à des verrous à crocheter, une activité très concrète symbolisant encore aujourd'hui un pan de la culture hacker. Dans toutes les grands-messes dédiées, comme *Le Hack* en France, on voit des stands consacrés au *lockpicking*, métaphore parfaite du défi technique à relever[208]. Seules règles à respecter néanmoins : on ne crochète que des serrures qui nous appartiennent et n'ont aucune utilité pratique. Cette lutte pour ou contre la gratuité du code informatique va accélérer les pratiques de *cracking*, le « vandalisme informatique » de ceux que les hackers du MIT appellent les « voleurs »[209].

Selon Steven Levy et les témoignages concordants de plusieurs spécialistes que nous avons interrogés, la communauté originelle du MIT va se fragmenter entre les partisans d'une approche mercantile exploitant les compétences spécifiques des hackers ou plus générales des informaticiens, et les défenseurs du logiciel libre et de la gratuité de l'information. Ce quatrième âge serait celui des derniers vrais hackers, représentés par le pionnier et militant du logiciel libre, Richard Stallman. L'on doit notamment à celui-ci les licences GNU/GPL (*General Public Licences*) visant à empêcher toute privatisation d'un logiciel libre pour en faire un produit qu'il qualifierait de « privateur »[210]. Ce positionnement avant tout politique,

[207] Rodrigo Nieto Gómez, *Ibid.*, p. 100.

[208] Outre les éditeurs de jeux vidéo, Microsoft notamment va mettre en place les premiers *Digital Rights Management* (DRM), lesquels vont favoriser l'utilisation du protocole de partage de fichier P2P FTP (*File Transfer Protocol*). En France au mois de septembre 2023, le « projet de loi visant à sécuriser et réguler l'espace numérique », s'il valide la disposition sur l'interdiction d'usage de VPN sur les RSN, risque pareillement de conduire à la constitution d'un marché noir de *proxies* sauvages. Beaucoup d'experts en cybersécurité et des hackers, tout en saluant d'autres propositions du texte par ailleurs, y sont défavorables.

[209] « *Thieves* ». http://tmrc.mit.edu/hackers-ref.html

[210] La suite bureautique *Libre Office* est une suite logicielle libre et ouverte qui est venue au secours du projet moribond *Open Office*. Un logiciel « privateur » est un produit propriétaire à code source fermé et protégé, comme la suite *Microsoft Office* par exemple. Richard Stallman est connu pour sa formule : « *Si je ne peux pas partager mes logiciels, alors j'ai l'impression de me couper du monde et de trahir la communauté des programmeurs.* »

souvent résumé par la philosophie du *copyleft* en opposition au *copyright*, s'accompagne de son pendant plus technique depuis 1998 : l'initiative *open source*[211]. Linus Torvalds, créateur du système d'exploitation (OS) Linux et promoteur de l'*open source*, explique : « *Les* hackers […] *se définissent comme des personnes qui "adorent programmer" et pensent que le partage de l'information est une chose extrêmement positive, et qu'il est* […] *de leur responsabilité éthique de partager leur expertise en développant des logiciels gratuits, en offrant un accès gratuit à l'information et à l'informatique chaque fois que possible.*[212] » Dans ce sillage, on l'a vu, les *cryptowars* et le mouvement *cypherpunk* vont s'inscrire dans le panorama de l'informatique grand public, au moment où la cryptographie devient à la fois un gage de confiance de l'espace numérique mais aussi une pratique conçue par les autorités gouvernementales comme source de dérives criminelles. Les deux manifestes *cypherpunk* se résument aux revendications et principes suivants :

- Nous avons tous quelque chose à cacher. Dire qu'on n'a rien contre la surveillance, car on n'a rien à cacher, c'est comme dire qu'on n'a rien contre la censure car on n'a rien à dire ;
- Protection de la vie privée et secret des communications ;
- Garantir l'anonymat numérique ;
- Combattre la censure et la surveillance ;
- Cacher qu'on se cache[213].

En 2013, l'anthropologue et professeure américaine spécialiste du cybermilitantisme Gabriella Coleman décrit son immersion dans les communautés de hackers et tire de l'expérience dans cet univers méconnu d'authentiques enseignements. Les principes sociopolitiques auxquels elles s'attachent sont les suivants :

- Protection de la propriété et des libertés civiles ;
- Protection de la tolérance et de l'autonomie individuelle ;
- Sécurisation d'une presse libre ;
- Direction via un gouvernement aux pouvoirs limités et des lois universelles ;
- Préservation du principe d'opportunité équitable et de méritocratie[214].

[211] https://opensource.org/

[212] Pekka Himanen, *L'éthique hacker et l'esprit de l'ère de l'information*, Exils, 2001, 219 p., p. vii. L'OS Linux est en réalité omniprésent, qu'il s'agisse des systèmes de serveurs, langages de programmation, le développement applicatif, le Web, équipements informatiques, les terminaux nomades avec Android, basé sur son noyau, etc.

[213] https://www.activism.net/cypherpunk/crypto-anarchy.html ; https://www.activism.net/cypherpunk/manifesto.html

[214] Gabriella Coleman, *Coding freedom: the ethics and aesthetics of hacking*, Princeton University Press, 2013, 254 p. Citée par Rayna Stamboliyska, *op. cit.*, p. 168.

Si le message paraît idéaliste et que les générations d'alors et *a fortiori* d'aujourd'hui ont un peu changé, l'éthique des hackers demeure. Bien qu'elle ait été probablement écornée ou dévoyée par le monde économique : on ne compte plus les utilisations du mot hacking devenu à son tour un produit (*growth hacking*, *crowd hacking*, *hackatons*…) mais avec parfois un fond d'authenticité préservé, cette éthique a en tout état de cause permis des avancées technologiques majeures sur lesquelles s'appuie aujourd'hui l'ensemble de la société : informatique, internet, cryptographie… D'aucuns considèrent même qu'Alan Turing est l'un des pères fondateurs du hacking. Mais pour les États, ces communautés peuvent porter atteinte à la sécurité, ou pour les entreprises nuire à leurs intérêts. Comme le note Rodrigo Nieto Gómez, « *les politiques de cybersécurité qui ont défini les cybermenaces n'ont pas reconnu ce lien entre le hacking et les capacités d'innovation, ni les lourdes conséquences économiques que le renforcement de la cybersécurité aura sur la créativité potentielle des entrepreneurs*.[215] »

Le mouvement des hackers s'apparente finalement à un Janus bifrons dont l'une des faces est orientée vers la liberté et la transgression, et l'autre vers une certaine conformité aux règles. Un cadre qui ne satisfait cependant pas les plus politisés d'entre eux.

### **2)** Typologie des hackers : *noirs*, *blancs*, *gris*

« *Tous les profils de hackers sont un peu bizarres. Jamais tout blanc ou noir. C'est une vision binaire qu'on a souvent.*[216] »

Pierre Penalba

Selon l'image d'Épinal consacrée, le hacker est un pirate informatique flanqué d'une capuche et enfermé dans sa chambre occupé à *cracker* des mots de passe sur l'Internet. C'est d'ailleurs devenu un jeu pour les principaux concernés – « éthiques » ou non –, qui ne sont pas les derniers à pratiquer l'autodérision voire la moquerie. En effet, si le hacking malicieux a débuté avec le *phreaking*, on peut considérer le *trolling* comme une de ses déclinaisons originelles. Les *trolls* informatiques sont des internautes cherchant à perturber les discussions sur les réseaux socionumériques, susciter l'attention par un comportement négatif, s'adonner à la raillerie ou à la pratique publique de ce que les Allemands appellent la *schadenfreude* : tirer du plaisir du malheur des autres et éventuellement les pousser à bout émotionnellement. Certains d'entre eux, sévissant sur des forums tels *4chan*, sont devenus plus tard des

[215] Rodrigo Nieto Gómez, *op. cit.*, p. 102.
[216] Entretien avec l'auteur, 07/07/2023.

hacktivistes[217]. Issus à l'origine des premières agoras de l'Internet comme les IRC[218] ou les forums, ils ont progressivement investi les RSN et glissé d'un *lulz*[219] aux mèmes sarcastiques jusqu'à se politiser avec l'ouverture du Web public. On leur doit également les pratiques de dessin électronique ou de proto-émoticônes basées sur l'encodage texte ASCII[220], le *leet speak* (substitution homogr4phique entre l3ttres et ch1ffres). Cette voie les a placés peu à peu en « hors-la-loi » tandis que les premiers criminels « augmentés » investissaient le cyberespace.


**Figure 11 :** *Typologie simplifiée des hackers*

Source : Yannick Pech, 2023 (iconographie libre de droit).

### a) *Les hackers noirs : des pirates informatiques illégaux*

La technologie n'est pas neutre. « *Internet est un* "pharmakon" » disait le philosophe Bernard Stiegler, empruntant à son confrère Jacques Derrida et lui-même à Platon[221]. L'espace

[217] Rayna Stamboliyska, *op. cit.*, pp. 173-185.
[218] *Internet Relay Chat*, les premières formes de messagerie instantanée textuelle sur l'Internet.
[219] Jeu de mots bâti à partir de l'expression « LoL » (*LaughOutLoud*). Un LoL grinçant et transgressif, entre humour noir et sadisme.
[220] Voir par exemple https://ascii-fr.com/
[221] https://www.espace-ethique.org/ressources/article/bernard-stiegler-un-homme-de-pensee-et-daction ; https://pharmakon.fr/wordpress/. Voir son approche pessimiste du numérique et de la technologie en général : Bernard Stiegler, *Ce qui fait que la vie vaut la peine d'être vécue. De la pharmacologie*, Flammarion, 2010, 272 p.

numérique est à la fois poison, bouc émissaire et antidote. À ce jeu de l'ambiguïté, le *chapeau noir* est délétère et on devrait plutôt le qualifier de forban numérique. « *Mais en informatique, c'est l'usage de la vulnérabilité qui fait la couleur du hacker*.[222] » Du moins, au regard du droit, car si l'on a compris un tant soit peu la philosophie des hackers, les critères du bien et du mal sont chez eux assez flous. C'est ce qui explique, nous le verrons, que l'épithète « éthique » assigné aux hackers blancs ne fait pas l'unanimité y compris chez ceux mêmes qui s'en réclament. Pour Philippe Truillet, le concept même de hacker est difficile à appréhender et le hacking *« c'est d'abord un jeu et du test radical ; disséquer les phénomènes, comprendre comment fonctionnent les machines*.[223] » Si les *black hats* originels se confondaient vraisemblablement avec les hackers responsables du MIT ou des *bidouilleurs* en quête de prestige, ils sont devenus des criminels guidés par l'appât du gain : escroquerie à la carte bleue ou usurpation d'identité de particuliers ; prise en otage et rançonnage de données volées aux entreprises ou collectivités ; piratage massif d'identifiants et mots de passe stockés dans des bases de données et monnayés sur le *darkweb* ; recherche de vulnérabilités (*o-day*) à exploiter mais surtout revendre au mépris des éditeurs de logiciels concernés… Cyberdélinquants rangés souvent parmi les *script kiddies*[224], cybercriminels, cyberterroristes, cyber-espions, hackers-corsaires représentent des sous-catégories malveillantes entrant dans le cadre des politiques de cybersécurité ou de cyberdéfense. Les hackers noirs sont aujourd'hui bien caractérisés par les instances et sujets légaux du droit.

### b) *Les hackers blancs : des attaquants légaux*

Bien sûr, le *chapeau blanc* est l'antidote du *pharmakon*, et l'analogie médico-biologique est poussée à son paroxysme quand on assimile ces hackers au système immunitaire du grand organisme numérique. Ces spécialistes de l'informatique travaillent contractuellement pour des organisations soit publiques soit privées ou par le biais de *bug bounty* en vue d'identifier leurs vulnérabilités. Le plus souvent autodidactes, ils ont appris en « bidouillant » et éprouvant le fonctionnement des machines et des logiciels pour atteindre, après beaucoup de travail et de persévérance, un niveau de connaissances leur permettant d'être reconnus comme hackers par leurs pairs[225]. En effet, le hacking est un milieu de cooptation plus que tout autre où on ne s'attribue pas soi-même le qualificatif. Les hackers forment *de facto* une sorte d'élite dont les seuls faits d'armes ont valeur de mérite, mais une élite informelle et non exclusive où n'importe qui peut s'illustrer dès lors qu'il apporte la preuve de ses compétences surtout techniques, mais

[222] Rayna Stamboliyska, *op. cit.*, p. 170.
[223] Entretien avec l'auteur, 15/09/2017.
[224] *Script kiddies* est une expression désignant littéralement les *gamins du code*, à savoir des non spécialistes qui, le plus souvent, achètent des *malwares* sur étagère sous forme de packs spécialisés en fonction des besoins.
[225] Selon Clément Domingo (entretien du 15/11/21), les « *vrais hackers* » sont des autodidactes et n'ont pas de diplôme d'ingénieur en sécurité informatique.

pas seulement. Par exemple, les aptitudes à l'ingénierie sociale sont très valorisées et souvent incontournables. La série *Mr Robot* en atteste, dont les protagonistes à la scène font très souvent appel à des méthodes de manipulation psychologique, tout comme les hackers à la ville. L'exemple le plus célèbre est celui de l'Américain Kevin Mitnick (2023†), souvent considéré comme l'un des meilleurs hackers au monde[226]. Ce savoir-faire global peut donc se décliner dans plusieurs domaines, d'où une grande variété de profils y compris chez les *chapeaux blancs* : spécialistes de rétro-ingénierie, *hardware*, intrusion physique, analyse forensique, programmation/codage, *pentesting* Web, traitement du signal (électromagnétique), cryptographie, stéganographie[227] et de plus en plus OSINT[228]. C'est valable pour tous les types de hackers, mais les *blancs* s'illustrent par des preuves de concept (PoC) lors de grands-messes dédiées, via les médias socionumériques ou des forums spécialisés, ou encore par le biais des scores et défis qu'ils remportent à l'occasion de compétitions appelées CTF (*Capture the Flag*[229]) ou dans le cadre de plateformes d'entrainement où sont émulés des systèmes d'information (machines virtuelles) que l'on doit compromettre (*pwning*[230]). Parmi les plus connues, l'on compte *Hack the Box* – la ou l'une des plus exigeantes –, *Rootme*, *TryHackMe*, *Pentesterlab* ou encore, pour débuter, *Yolospacehacker*.

Toutefois, le traitement médiatique et politique de ce statut de *hacker blanc* divise, donnant lieu à une controverse sur l'usage du qualificatif « éthique ». Enseignant à SciencePo, entrepreneur et esprit critique acéré, Fabrice Epelboin propose le premier contre-champ à une expression dont il dit qu'elle a été inventée par IBM. Selon lui, « *C'est un hacker qui travaille au service d'une entreprise et pas au service d'une cause morale. Il respecte juste la loi*.[231] » Pour sa part, le hacker Alexandre « Maître » Oda parle d'une expression « *un brin*

[226] L'un de ses ouvrages de référence traite d'ailleurs de cette question ; Kevin D. Mitnick, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2003, 368 p.
[227] Science et art de la dissimulation d'une information. Par exemple, l'incorporation d'un texte dans une image (via un pixel par exemple, qui contient une valeur de couleur codée sur plusieurs bits – technique dite « bit de poids faible » (LSB)). À la différence de la cryptographie, l'objectif n'est pas de chiffrer mais de cacher un élément.
[228] Plusieurs témoignages d'entretiens vont dans ce sens. L'OSINT est assimilé à du hacking pour deux raisons : ses techniques sont utilisées dans la méthodologie de travail des hackers ; et l'état d'esprit qui y préside, celui de l'effort, de la patience et de l'ingéniosité, est souvent associé à celui du hacking (entretiens avec Clément Domingo (15/11/2021), Sylvain Hajri (27/02/2023), Julien Métayer (30/03/2022), Florent Curtet (30/09/2021)…
[229] « *Jeu consistant à exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer les drapeaux, preuves de l'intrusion* » selon la plateforme spécialisée *Rootme* (https://www.root-me.org/). Par exemple le CTF404, parrainé par la DGSE, qui se tient en France depuis 2022 (https://web.archive.org/web/20220521090918/https://ctf.404ctf.fr/) ou encore le DG'hAck organisé par la Direction générale de l'armement (DGA, https://www.dghack.fr/).
[230] De « *pwn* », néologisme argotique usité chez les *gamers* et les hackers. Il aurait été inventé sur la base d'une erreur de frappe (*pwned*/*owned*) et signifierait donc *perfectly own* (posséder parfaitement), c'est-à-dire vaincre son adversaire.
[231] Entretien avec l'auteur, 08/04/22.

*marketée*[232] » qui recoupe toutefois plusieurs types de hackers, des *pentesters* dont certains peuvent travailler avec le gouvernement. L'on pourrait faire remarquer qu'une éthique n'est pas nécessairement un code moral, mais plutôt un ensemble d'us et coutumes à vocation fédératrice ; ce que forment dans une certaine mesure les communautés dites de « hackers éthiques » en France. De manière plus catégorique, « Alice[233] » affirme que « *les blancs ne sont pas des hackers*. » Cette position rejoint quelque peu les propos de l'ancien directeur de l'ANSSI qui, s'il *« est de bonne constitution, mais* [*il*] *applique des dogmes*.[234] » selon Florent Curtet, confirme : « *il n'y a pas de tout blanc ou de tout noir chez les hackers. Mais il y a des limites à ne pas franchir. D'un autre côté, chez les hackers eux-mêmes, ceux qui refusent la catégorisation* [noir/blanc/gris]*, ils jouent un jeu extrême.* [235] » Ce jeu est précisément souvent le fait des *chapeaux gris*, dits aussi « hacktivistes ».

### c) *Les hackers gris : des justiciers alégaux ?*

Dans notre *pharmakon*, l'hacktiviste est-il le *bouc-émissaire* ou un vrai *pharmakós* du cyberespace ? En vertu d'une cause qu'ils qualifient généralement de supérieure, les hackers gris vont agir au-delà du simple militantisme et outrepasser les lois et règles communes. Le terme est ainsi un mot-valise formé de « hacker » et « activiste ». La démocratisation de l'accès à l'Internet a permis la formation de groupes qui, sans même se connaître, se sont unifiés de manière circonstancielle ou plus pérenne. Les mouvements politisés de militants se sont donc rapidement emparés du Web *social*, devenu modèle et lieu de coopération décentralisée[236]. Sur la base du principe reconnu de la dynamique de groupe, les militants les plus actifs sont forces de projets, qu'ils peuvent lancer dans le cadre d'une cause fédératrice dont sont solidaires les autres membres du collectif. De fil en aiguille, plusieurs mouvements issus d'abord des forums puis des réseaux socionumériques ont émergé et se sont densifiés dans des organisations où la *do-ocratie*, le pouvoir de « celui qui fait qui a raison[237] » est moteur de l'action autour d'une cause commune. Dans sa thèse de doctorat, Alexandra Samuel définit l'hacktivisme comme « *l'utilisation non violente d'outils numériques illégaux ou juridiquement ambigus à des fins politiques*.[238] » Bien entendu, le principe de légitimité est central dans l'action des hackers gris, dont « Alice » estime qu'ils ne « *peuvent pas être "blancs"*.[239] »

[232] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.
[233] « Alice » sera le pseudo attribué à une hackeuse se disant sans « couleur », mais pouvant être considérée comme une *hacktiviste* (« hackeuse grise »).
[234] Entretien avec Florent Curtet, 30/09/2021. Ancien *black hat*, Florent Curtet est devenu hacker *éthique*.
[235] Entretien avec Guillaume Poupard, 17/04/2023.
[236] Naomi Klein, *No Logo : La tyrannie des marques*, Babel, 2002, 752 p.
[237] Emmanuel Bloch, *op. cit.*, p. 84.
[238] Alexandra W. Samuel, *Hacktivism and the future of political participation*, Université de Harvard, 2004, cité *in* Emmanuel Bloch, *ibid.*, p. 85.
[239] Entretien avec l'autrice, 01/03/2023.

Le rapport à cette légitimité se manifeste dans l'usage de techniques plus que d'outils, comme par exemple les attaques par *déni de service* (DOS) qui forment le principal moyen de s'opposer à une organisation. Mais tous les hacktivistes n'approuvent pas forcément cette façon de faire. Par exemple, elle a été la technique la plus utilisée par les *Anonymous* dans les années 2010, qui l'assimilaient au principe des manifestations et *sit-in* numériques. Tandis que le collectif des *Telecomix* en condamnait l'usage car ils l'estimaient contraire au principe de libre circulation de l'information[240]. Dans la lignée de ces mouvements, plusieurs collectifs se sont aujourd'hui structurés en associations spécialisées dans l'investigation afin de servir des causes politiques ou humanitaires. C'est le cas de l'ONG Disclose[241] qui a enquêté sur plusieurs affaires liées à la politique étrangère française, dont celle du détournement par l'État égyptien du renseignement fourni par la DRM à des fins de ciblage de criminels de droit commun en lieu et place de profils terroristes, en vertu d'un accord *offset*[242] conditionné à l'achat d'avions de combat Rafale. Ou encore le cas de la publication d'une note confidentielle du même service de renseignement (SR*) français faisant part aux décideurs politiques de ses préoccupations concernant les enquêtes d'ONG sur le théâtre yéménite visant à prouver que l'État français, partie à un accord international de 2014 interdisant aux gouvernements signataires de vendre des armes à des États en guerre, avait poursuivi ses exportations. La question centrale était de savoir si la France avait honoré son engagement car des armes/munitions françaises ont été utilisées par l'Arabie saoudite contre le gouvernement yéménite houthiste.

Si les ONG, les activistes et leur combat pour des causes réputées humanistes et « hautement morales » peuvent être tout à fait critiquables, l'inversion des valeurs cardinales des sociétés démocratiques opérée depuis quelques décennies et accélérée par la montée en puissance des RSN concourt à légitimer leurs actions. Si notamment le critère de vérité est remis en cause et de plus en plus concurrencé par celui de popularité, alors les critères fondant la légitimité sont pareillement soumis à de multiples fluctuations. Selon Philippe Truillet, les hacktivistes peuvent à la fois vouloir participer à « *désintoxiquer de certaines manipulations – le marketing, c'est de la manipulation ! – mais ils récupèrent les outils numériques et réutilisent l'information, et deviennent souvent eux-mêmes sources d'une nouvelle*

[240] Voir Emmanuel Bloch, *op. cit.*, et Rayna Stamboliyska, *op. cit.*, pp. 180-198.

[241] https://disclose.ngo/. Fin septembre 2023, la journaliste chargée de l'enquête a été mise en garde à vue par suite de deux plaintes déposées par le MINARM. Elle est accusée de « compromission du secret de la défense nationale et révélation d'information pouvant conduire à identifier un agent protégé ». Sa source principale, un lanceur d'alerte, s'avèrerait être un ancien fonctionnaire du ministère.

[242] Un accord *offset* consiste, dans le cadre d'une transaction commerciale, à ajouter des clauses compensatoires au contrat d'achat en faveur du client. Cela peut prendre la forme de menus services, de co-entreprises, de transferts de technologies ou de savoirs pouvant se révéler du reste très préjudiciables en termes de compétitivité. En 2016 par exemple, l'achat par l'Inde de 36 Rafale a été notamment conditionné à une délocalisation vers le Bharat d'une partie de la fabrication des exemplaires de l'avion de combat.

*intoxication, extrémiste, à l'envers, via ce que l'on appelle la réinfosphère.*[243] » Par ailleurs, les lanceurs d'alerte peuvent être apparentés à des hacktivistes, puisque leurs motivations profondes restent ambiguës, sans compter qu'au même titre que ces derniers ils outrepassent la loi ou le secret des affaires. Les *Anonymous* ont du reste participé à la campagne « *Avenge Assange* » lorsque celui-ci a fait l'objet d'un mandat d'arrêt international émis par la Justice américaine. Pour Cédric Perrin, les hacktivistes restent cohérents avec un certain code d'honneur, lequel s'aligne toutefois sur le sens de la cause qu'ils défendent[244]. Certains hacktivistes partagent en outre des communautés de pratiques avec les SR et l'intelligence économique, mais pas avec les mêmes résultats, selon le lieutenant-colonel Leberon[245]. D'une manière générale, la position de l'hacktiviste fait écho à l'aphorisme du stoïcien Sénèque quand il dit, en substance, que la raison veut décider de ce qui est juste tandis que l'émotion veut qu'on trouve juste ce qu'elle a décidé.

Si l'on tente de dresser le portrait type du hacker, parmi ces multiples nuances ici simplifiées et d'après nos observations, certaines caractéristiques peuvent être dégagées :

| **Caractères communs aux hackers** |
|---|
| Principes de liberté et d'ouverture |
| Valeur du partage et esprit communautaire |
| Sens du défi et du jeu |
| Goût du risque/de l'interdit |
| Anticonformisme et iconoclasme |
| Patience et opiniâtreté |
| Philosophie du RTFM et de la « débrouille » |
| Goût de l'effort et du dépassement (dans leur domaine) |
| Créativité et curiosité |
| Inclination à la pensée alternative (*think out of the box*) |
| Passion et humilité |
| Besoin de reconnaissance, accessibilité et attitude détendue |
| « *Borderline, geek, Asperger voire plus* »[246] |

**Figure 12 :** *Essai de caractérisation des hackers*

Source : Yannick Pech, 2023. Basé sur nos observations et les témoignages de hackers.

[243] Entretien avec l'auteur, 15/09/2017. Un lanceur d'alerte comme Edward Snowden, bien qu'il ait pu vouloir se placer sous les feux des projecteurs, a vraisemblablement connu une profonde dissonance cognitive et éthique. C'est ce que suggère ses *Mémoires vives*, Seuil, 2019, 384 p. Plus controversé, le cas Julian Assange, s'il illustre ce dilemme du besoin de reconnaissance, montre toutefois qu'un lanceur d'alerte peut subir un traitement particulièrement sévère dans le cadre de procédures judiciaires émanant pourtant d'États démocratiques.
[244] Entretien avec l'auteur, 05/10/2017.
[245] Entretien avec l'auteur, 21/06/2017.
[246] Des mots de Florent Curtet (entretien du 30/09/2021, et *Hacke-moi…*, *op. cit.*).

## **B.** *Des communautés de hackers ?*

*Nous sommes les Hackers, les tâcherons de l'abstraction, à la fois les bousilleurs et les novateurs – les dépeceurs, les limiers d'univers. Nous produisons de nouveaux concepts, de nouvelles perceptions, de nouvelles sensations, hackées à partir de données brutes. Quel que soit le code que nous hackons, serait-il langage de programmation, langage poétique, mathématique ou musique, courbes ou couleurs, nous sommes les extracteurs des nouveaux mondes. Que nous nous présentions comme des chercheurs ou des écrivains, des artistes ou des biologistes, des chimistes ou des musiciens, des philosophes ou des programmeurs, chacune de ces subjectivités n'est rien d'autre qu'un fragment de classe qui advient peu à peu, consciente d'elle-même.*

McKenzie Wark

Le propos est affable : « *Le hacking au sens large, c'est : tu trouves un problème, que tu résous de manière élégante en pensant* out of the box.[247] » Telle pourrait être la vision des hackers informatiques. À ceci près que cette approche est précisément trop élégante pour correspondre à la maxime *Quick & Dirty* propre aux hackers originels. On bricole vite fait, on place un « bout de sparadrap », un *patch*, et on reviendra régler le problème de manière plus assurée et approfondie plus tard. Surtout, le hacking n'est pas l'apanage d'informaticiens spécialisés dans la sécurité et le fonctionnement des ordinateurs. Plusieurs formes ou nuances de personnalités peuvent disposer de l'état d'esprit et surtout de l'éthique des hackers. C'est pour cette raison que le hacking est avant tout un mouvement intellectuel et politique. Demeure toutefois une ambiguïté sur son origine, puisque le mot hacker préexistait avant l'appropriation qu'en ont fait les étudiants du MIT de Boston à la fin des années 1950. McKenzie Wark fait d'ailleurs valoir que le hacker tient autant du bucheron qui élague les arbres que de l'explorateur des entrailles numériques[248]. Pour Manuel Castells, professeur de sociologie spécialiste de la Silicon Valley, ce développement ne touche pas seulement une communauté numérique, mais aussi les grandes couches sociales, politiques et économiques. Quant au philosophe Pekka Himanen, il voit les hackers comme des « *citoyens modèles de l'ère de l'information.* [...] *les véritables moteurs d'une profonde mutation sociale. Leur éthique, leur rapport au travail, au temps ou à l'argent, sont fondés sur la passion, le plaisir ou le partage. Cette éthique est radicalement opposée à l'éthique protestante, telle qu'elle est définie par Max Weber, du travail comme devoir, comme valeur en soi, une morale qui domine encore le monde aujourd'hui.*[249] » En un sens, l'état d'esprit du hacking peut concerner tout un chacun.

[247] Interview de Victor Poucheret, chaine *Thinkerview*, *op. cit.*

[248] Par ailleurs, depuis les années 2000, on parle d'une nouvelle communauté désignée sous le nom de *biohackers*, car ses membres essaient de manipuler le vivant dans une logique transhumaniste.

[249] Pekka Himanen, *op. cit*., p. 52.

Cette vision élargie se retrouve dans le célèbre *Manifeste du hacker* de Loyd Blankenship dont le message revêt une dimension éminemment sociopolitique. On a parlé des « hackers-libertaires » et des « hackers-privateurs » ; des chapeaux blancs, des chapeaux noirs et gris. Dans l'univers et l'acception informatiques du mouvement, cet héritage est immanent aux hackers modernes puisque, on l'a vu, cela a contribué à les scinder en plusieurs branches ou peut-on dire communautés. Le sujet se prête particulièrement à la médiologie, surtout en ce qui concerne les hackers informatiques, à l'interface de la technique et d'une contre-culture. D'ailleurs, pour Philippe Truillet, la logique communautaire du « hack » tend à se diluer dans la société pour favoriser plus d'intelligence collective et ainsi régler des problèmes en tous genres. « *Ça crée ou recrée du lien social. C'est une logique virtuelle à la base (communauté de gamers, de bidouilleurs, etc.), puis aujourd'hui il y a une reterritorialisation avec les fablabs. Le numérique recrée presque du lien social dans le contexte de son délitement*.[250] » Ainsi, une communauté de hackers « puristes » très attachés aux libertés et à une philosophie de l'ouverture ; une autre préoccupée davantage par un besoin de reconnaissance légale et ainsi possiblement plus adaptée au temps où, au-delà des pieux principes, le hacking s'est lui aussi marchandisé. Comme le souligne Julien Métayer, certains hackers – comme lui dit-il – prennent notamment le parti d'être « communiquant ». S'il existe par conséquent une multiplicité de profils, l'on peut considérer que plusieurs communautés coexistent qui partagent finalement les mêmes principaux caractères. Demeure néanmoins une certaine nuance et un débat sémantique sur d'un côté, les spécialistes qu'on qualifie de défenseurs (*blueteamers*) et ceux dont le *mindset* est plus fidèle à l'approche d'un attaquant *(redteamers*) de l'autre. Un débat qui trouve ses racines dans les rapports houleux qui ont initialement lié les hackers et les institutions publiques ou privées.

### **1)** Communautés, individualités, liens initiaux avec les autorités

Pour Clément Domingo, dans la perspective étatique française, on ne travaille pas directement avec des hackers ; « *officiellement, il n'y a pas de hackers*.[251] » Cependant que les entreprises font affaire avec des ingénieurs en cybersécurité pouvant éventuellement faire du *pentesting* ou du *redteaming*[252], mais qu'elles n'appréhendent pas vraiment comme des hackers. Ainsi entretiennent-ils des rapports, d'une part, plus normalisés par simple

[250] Entretien avec l'auteur, 15/09/2017.
[251] Entretien avec l'auteur, 15/11/2021.
[252] Le *redteaming* diffère du *pentesting* dans l'objectif d'un test d'intrusion. Là où un pentester doit exhaustivement détecter et rapporter les vulnérabilités à son client, le *redteamer* cherche surtout à identifier la faille principale et la plus critique d'un SI. Les tests d'intrusion physique sur site sont aussi plutôt le fait de *redteamers*. Enfin, généralement, le *pentester* a accès à plus de contexte et de ressources sur sa cible (tests *white/grey box*), et les équipes de défenseurs (*blueteamers*) ne sont pas mis au courant lors des tests d'intrusion *redteam.*

pragmatisme, les organisations privées comprenant de mieux en mieux les enjeux de sécurité ; mais ces liens en réalité encore distants témoignent des difficultés encore nombreuses et du temps que « *cela va leur prendre* [pour] *embrasser la culture hacker, de chaos créatif*.[253] » En fin de compte, les communautés de hackers se distinguent surtout par l'intention qui les anime au-delà d'un état d'esprit commun. Cet écosystème en soi est extrêmement complexe selon les mots de Victor « Doomer » Poucheret, pour qui plusieurs communautés coexistent en fonction de savoir-faire spécifiques, « *de compétences classiques type SSI/cybersécurité, l'offensive et les "vrais" hackers, la "bidouille" technique ou physique*. » Ces communautés sont visibles sur les RSN poursuit-il, « *Discord, Twitter, LinkedIn* » sur lesquels « *beaucoup de discussions ont lieu et on reste sur les pseudos. C'est un monde assez petit. On se connait tous plus ou moins, de près ou de loin*.[254] »

### a) *Une communauté composite*

Ce *mindset* du hacking est transposable à d'autres domaines que l'informatique, on l'a vu. Le principe fondamental consiste à solutionner des problèmes en faisant plus avec moins, en étant capable d'aborder les choses autrement et de manière créative. Brice Augras emploie l'expression « d'Ikea bidouille » pour qualifier cet état d'esprit[255]. Les hackers se cooptent et se font « baptiser » par leurs pairs, ajoute Alexandre Oda[256]. Pierre Penalba parle d'une « *vraie communauté* » de hackers éthiques en France, « *qui revendique une pureté originelle* (sic)*, c'est-à-dire qui n'a jamais commis de péchés, versé dans l'illégal*.[257] », contrairement aux hacktivistes et bien sûr aux cybercriminels. Leurs homologues éthiques, tout en condamnant ces derniers font toutefois preuve d'une certaine mansuétude à leur égard, comme plusieurs témoignages l'attestent. Cette communauté « éthique », poursuit Pierre Penalba, n'est pas celle des experts classiques de la cybersécurité car ils utilisent l'offensif. Dans la même optique, Victor Poucheret estime que le cadre juridique en France pose un problème d'adaptation avec la communauté du hacking, sans doute parce que dès lors qu'on parle de hacker éthique, « *la cybersécurité plus classique n'est jamais loin*. » En fait, entre hacker et « expert cyber », nous observons que la frontière semble de plus en plus ténue, au risque peut-être que le profil originel du hacker se galvaude. Ceci peut s'expliquer par le long combat qu'ont mené les hackers français pour être reconnus par des autorités longtemps restées méfiantes sinon hostiles. L'histoire de leurs rapports a en effet très mal commencé.

[253] Entretien avec Victor Poucheret, 14/11/2021.
[254] *Idem.*
[255] Interview de Brice « Zax » Augras, *Thinkerview*, *op. cit.*
[256] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.
[257] Entretien avec l'auteur, 07/07/2023.

### b) *Un traumatisme originel en France*

« *Ça a mal commencé* » déplore Fabrice Epelboin. Tout est parti d'un péché originel commis par la DST, l'ancêtre de la DGSI. Déjà peu en odeur de sainteté, les hackers français vont vivre comme une trahison de l'État le stratagème échafaudé par le service du ministère de l'Intérieur à la fin des années 1980. À cette époque, un groupe d'hacktivistes d'Outre-Rhin se structure pour devenir une vraie tribune politique discutant avec les autorités allemandes. Ce collectif, considéré comme le premier groupe de hackers au monde, est baptisé le Chaos Computer Club (CCC*) et a toujours pignon sur rue de nos jours. Selon le journaliste d'investigation Jean-Marc Manach, le CCC a aidé la Stasi est-allemande à mieux appréhender l'opération psychologique menée par les États-Unis à la fin de la guerre froide pour duper les Russes[258]. Appelée officiellement *Initiative de défense stratégique* (IDS) mais rebaptisée « guerre des étoiles » par les médias, elle formait un projet de bouclier antimissiles parfaitement irréalisable à l'époque. L'objectif consistait à intoxiquer l'URSS en vue de sa dislocation en l'entrainant dans une course scientifique vouée à l'échec.

En 1989, la DST est en train de se numériser et fait alors appel à des étudiants en informatique parfois hackers dans le cadre de leur service militaire. Elle subodore le rôle potentiel qu'ils pourraient jouer mais aussi la voie illégale qu'ils pourraient emprunter. Dès lors, le service monte une opération pour cartographier la communauté des hackers français en créant un véritable cheval de Troie, un Chaos Computer Club France (CCCF) inspiré de celui de Hambourg[259]. Le faux nez – ou *honeypot* dans le langage informatique – est de surcroît dirigé par Jean-Bernard Condat, un des hackers français les plus en vue au début des années 1990. Mais il travaille en réalité pour la DST depuis 1982. Comme le dit un proverbe arabe, *c'est de la confiance que naît la trahison*. Les hackers français vont ainsi très mal digérer ce camouflet et accuser les autorités d'être antipatriotiques[260]. Pour Olivier Laurelli, « *c'est l'événement traumatique des rapports entre autorités et hackers. Même si la génération de hackers actuelle ne le sait plus ou rarement. Il y a un niveau historique et culturel de défiance*.[261] » Selon lui et Fabrice Epelboin, c'est à ce moment-là que les hackers français se sont divisés, dont beaucoup d'entre eux ont rejoint la communauté du logiciel libre voire l'Allemagne, « *mais aucune association de hackers n'a été créée en France qui aurait pu être un interlocuteur de l'État, contrairement à l'Allemagne avec le CCC*.[262] » Fabrice Epelboin fait valoir que le CCC de Hambourg a créé une « *véritable synergie avec l'État* » allemand, « *cela*

[258] Entretien avec l'auteur, 10/04/2023.
[259] Sylvain Bergère, *Une contre-histoire de l'internet*, *op. cit.* Fait remarquable, à l'époque l'officier de police Pierre Penalba est à la fois partie prenante et contradicteur du projet CCCF (entretien avec l'auteur, 07/07/2023).
[260] Entretien avec l'auteur, 08/04/2022.
[261] Entretien avec l'auteur, 30/03/2023.
[262] Entretien avec l'auteur, 08/04/2022.

*fait un moment que les hackers sont entendus, consultés, reçus.* […] *Le législateur va voir les hackers au préalable, discutent avec eux, consulte leur point de vue. Il y a une vraie collaboration.* » Yassir Kazar, directeur de Yogosha, se rallie à ces propos et présente le CCC comme « *un vrai interlocuteur face à l'État* […] *qui a réussi à s'imposer*.[263] »

Or, les autres « apatrides » de la communauté française originelle vont parfois emprunter des voies criminelles, en basculant dans la piraterie informatique. À cet égard, le témoignage de Victor Poucheret est révélateur. Sans excuser ces agissements mais en présentant les choses de manière moins manichéenne, ce dernier évoque l'importante frustration voire le dégoût ressentis par de nombreux hackers. Certains n'avaient aucun repère et ne savaient quoi faire de leurs compétences. Jusqu'en 2016, les remontées de failles, toujours très encadrées aujourd'hui, étaient impossibles alors qu'elles procédaient d'une intention louable. Cette impression d'évoluer au sein de cadres étroits expliquera en partie la trajectoire de Florent Curtet, comme nous le verrons plus loin. Alexandre Oda, quant à lui, livre une anecdote personnelle intéressante, sur le jeune apprenti qu'il avait pris sous son aile. Ce dernier virerait en effet de bord en l'informant qu'après avoir bien appris à ses côtés, il allait passer du « *côté obscur* »[264]. Au-delà de l'analogie avec la saga *Star Wars* souvent convoquée par les principaux intéressés, le pseudonyme (« cre$us ») de ce hacker en herbe annonçait peut-être un destin déjà tracé. Alexandre Oda en a conçu une forte déception puisqu'il dit ne plus souhaiter accompagner de nouveaux disciples.

### c) *Des initiatives pourtant prometteuses…*

Dans le même temps, passé l'âge obscur des années 1990, les initiatives personnelles au sein de la DST ou de la DGSE sont prometteuses. Notamment, le directeur scientifique du service policier, Jean Guyaux dit « La baleine » va prendre les devants et recruter une dizaine de « baleineaux », des hackers hexagonaux[265]. Deux critères de sélection y président : la compétence et le sens de l'humour, car « *plus ils savaient rigoler, plus ils étaient sérieux pour moi. Parce qu'il faut être fou pour faire ces choses… Il faut s'amuser !* [266] ». Tandis que son homologue de la direction technique de la DGSE, Bernard Barbier, s'entoure de ses propres hackers dans les années 2000. Aujourd'hui, le SR extérieur propose des offres d'emplois dans l'offensif, comme l'atteste cette capture d'écran issue de son compte LinkedIn.

[263] Entretien avec l'auteur, 20/05/2022.
[264] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.
[265] Général Jean Guyaux, *L'espion des sciences*, Flammarion, 2002, 360 p.
[266] Sylvain Bergère, *Une contre-histoire…*, *op. cit.*

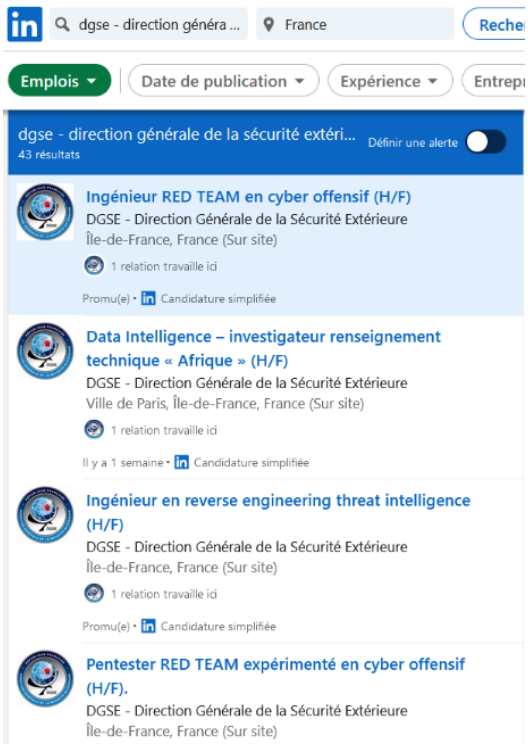



**Figure 13 :** *Capture d'écran des offres d'emplois publiées par la DGSE en juillet 2023*

Source : Réseau socionumérique professionnel LinkedIn.

Plus tard, l'ancêtre du FIC est fondé en 2003 par Frédéric Raynal, un ami d'Éric Filiol et fondateur des médias *MISC* et *reflets.info* et de la société Quarkslab[267]. De son acronyme le SSTIC[268], cette conférence annuelle toujours active réunit des passionnés et experts issus de divers horizons s'intéressant aux aspects scientifiques et techniques des TIC et de la sécurité de l'information. Universitaires, fonctionnaires, journalistes, informaticiens… Parmi eux, le groupe RSTACK se distingue par ses hackeurs brillants dont Laurent Oudot, cofondateur de l'entreprise de cybersécurité TEHTRIS et ancien de la DGSE où il a rencontré son associée Éléna Poincet[269]. Dans ce sillage, à la fin des années 2000, Philippe Langlois crée le premier *hackerspace* en France après avoir fondé l'une des premières entreprises de cybersécurité en 1995, Intrinsec[270]. Par ailleurs, la décennie 2000 voit émerger un haut représentant à l'intelligence économique, Alain Juillet, à qui on crédite d'avoir opéré un rapprochement avec les hackers, tandis que le deuxième directeur de l'ANSSI (2014-2022), Guillaume Poupard, est

[267] Entretien avec Jean-Marc Manach, 10/04/2023. https://connect.ed-diamond.com/misc ; https://www.quarkslab.com/fr/a-propos/ ; https://reflets.info/ (cofondée avec Olivier Laurelli).
[268] Symposium sur la sécurité des technologies de l'information et des communications (https://www.sstic.org/).
[269] Entretien avec Jean-Marc Manach, 10/04/2023. https://tehtris.com/.
[270] Les *hackerspaces* sont des laboratoires communautaires ouverts où les hackers peuvent partager leurs ressources et leurs connaissances (https://www.tmplab.org/) ; https://www.intrinsec.com/

célébré pour son volontarisme et son ouverture d'esprit[271]. Malgré ces avancées, beaucoup de hackers ou de spécialistes cyber pointent des manquements d'un point de vue politique et des disparités certaines au sein des communautés plutôt que de la communauté du hacking.

#### d) *… Mais tardives et insuffisantes*

En 2013, Éric Filiol déplorait : « *Le problème, c'est que la France a longtemps diabolisé les hackers.*[272] » On a parlé du puissant mépris qu'ont nourri nombre de hackers français pendant des années. Certains ont même quitté la France pour rejoindre l'Allemagne et le CCC car ils avaient des desseins démocratiques. Mais d'autres sont partis rejoindre des États qui l'étaient bien moins, comme l'atteste Alexandre Oda : « *Entre 2015 et 2017, il y a eu une grande vague de recrutement des hackers dans le monde par la Russie* […]. *Ils repéraient des personnes actives et compétentes sur des forums pour leur proposer du travail* […]. *Moi, à ce moment-là, j'ai vu des hackers français très bons partir en Russie.*[273] ». Et d'ajouter : « *En 2017 j'ai commencé à dire aux gens, vous allez voir, aujourd'hui les gens n'en ont rien à cirer, on nous prend pour des rigolos, des geeks, mais demain les entreprises vont courir pour venir nous recruter.* » Des propos corroborés par Clément Domingo ou Damien Cazenave, pour qui **les meilleurs hackers français sont partis pour cause de mauvaise valorisation à tous points de vue**[274]. En outre et en dépit de l'image positive dont est auréolée la communauté des hackers, l'esprit de camaraderie a ses limites, et un hacker reste souvent un électron libre y compris vis-à-vis de ses pairs.

### 2) Cyberattaquants et cyberdéfenseurs : un même objectif, une autre approche

Si l'on reconnait généralement aux hackers une forme de sociabilité sélective qui les réunit dans une ou *des* communautés, ces profils sont avant tout des individus qui interagissent par émulation, passion commune et sens du partage mais aussi par compétition. Les propos suivants de Victor Poucheret sont intéressants à ce titre : « *L'outil le plus important c'est ton état d'esprit, la manière de penser et de t'approprier ce qui a été créé par la communauté. Une fois que tu t'es approprié tout cela, soit tu utilises tes propres outils, soit tu utilises ce qui est déjà existant pour ne pas réinventer la roue.*[275] » On peut ainsi les lire à travers plusieurs prismes. Par exemple, on a parlé de profils plus communicants que d'autres ; à travers nos observations, nous avons pu voir évoluer certains profils volontiers discrets produire

[271] Entretien avec Clément Domingo, 15/11/2021.
[272] https://www.lemonde.fr/blog/bugbrother/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/
[273] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.
[274] Entretiens avec Clément Domingo, 15/11/2021 et Damien Cazenave, 24/07/2017.
[275] Interview de Victor Poucheret et Brice Augras, *Thinkerview*, *op. cit.*

davantage de publications sur les réseaux socionumériques professionnels, avec un souci évident de se rendre plus visibles. Entre passion du sujet et valeur de partage, et volonté voire nécessité d'élever leur audience, il est difficile de juger. Il ne faut pas oublier qu'une grande majorité des hackers est indépendante et s'évertue à le rester. Même si les témoignages recueillis et les autorités comme l'ANSSI signalent généralement la pénurie de spécialistes, on note que les hackers temporisent souvent en spécifiant que la concurrence entre eux n'a pas lieu d'être[276]. De la même manière, pour « exister » dans la communauté, il vaut mieux publier des résultats, faire état de prouesses techniques démontrées lors des challenges dédiés. Tout ceci amène à gagner en notoriété. Dans le cadre de CTF organisés par des organismes publics par exemple, et même si le côté bon enfant l'emporte très largement, le score compte. Lors de ce genre d'évènements, certains participants n'hésitent pas à annoncer que l'organisme en question les a contactés, avec parfois pour les plus indépendants une certaine forme de dédain, sans qu'il soit vraiment facile de savoir s'il était feint ou sincère[277].

En contre-champ de l'esprit de partage caractéristique de cette communauté, Julien Métayer nuance en précisant qu'il n'y a pas de partage de savoir-faire entre hackers légaux, contrairement à ce qui se passe entre hackers noirs[278] et aux États-Unis où, dit-il, « *il y a beaucoup de clubs de hackers, avec un esprit collaboratif, qu'on n'a pas en France.* », rejoignant par-là l'avis de Fabrice Epelboin. « *Il y a un début de rapprochement,* poursuit-il, *mais ça reste une coquille vide, et c'est à but politique/militant, avec Hackers sans frontières par exemple.* » Selon lui, les CTF tenus en « présentiel » ou les grands-messes comme *Le Hack* leur permettent de se rencontrer en vrai et d'apprendre à se connaitre. Mais sans échange de pratiques et sans projet concret collectif. Il conclut : « *Il y a une séparation vie publique/privée et* […] *une grosse défiance vis-à-vis du statut autoproclamé de "hacker". Il y a un côté "chacun pour soi".*[279] »

### a) *Une dilution de la figure du hacker ?*

On l'a dit, la frontière entre les différents profils de hackers est passablement brouillée. Cela pose la question de savoir si la figure du hacker ne s'est pas étiolée ou galvaudée. Du fait même de la tendance actuelle à justement en faire un acteur « éthique », peut-on toujours parler de vrais hackers et pas parfois, au mieux, de spécialistes de cybersécurité classiques, au pire de pseudo-experts ? Nombre de hackers se plaignent en effet de ce que le « cyber » est

[276] C'est le message véhiculé par exemple par Victor Poucheret et Brice Augras (interview *in Thinkerview*, *op. cit.*)
[277] Ces constats se basent sur nos observations *in situ* puisque nous avons participé à certains CTF. Nous ne mentionnerons ni lesdits individus, ni lesdits évènements.
[278] Entretien avec l'auteur, 30/03/2022. Ce dernier a 47 ans. Des hackers plus jeunes ne tiennent souvent pas le même discours.
[279] Entretien avec l'auteur, *ibid.*

devenu un « *buzz word bullshité, un terme fourre-tout* », évoquant comme Victor Poucheret « *la transition du milieu du hacking et donc de la cybersécurité et l'aspect business qui en découle aujourd'hui. Si tu fais rentrer de la gloire et de l'argent dans un milieu, forcément tu as cette transformation d'un milieu qui était initialement beaucoup plus communautaire,* open*, et bon il n'y a pas forcément réellement d'argent à se faire donc on est… tous copains. À un milieu où effectivement, on a des exigences en termes de business,* sponsorship *et marketing*.[280] », milieu qui a servi de prétexte à beaucoup de prestataires sans réelle qualification pour s'engouffrer dans la brèche d'un nouveau marché.

### b) *Attaquant ou défenseur : deux états d'esprit différents*

Nos observations nous inclinent à **poser comme hypothèse que, sous l'effet de l'environnement économique et des enjeux de la numérisation de la société, une hybridation s'opère insensiblement entre le profil des hackers dits éthiques et celui des experts en SSI**. Leur savoir-faire technique en constitue par ailleurs un autre facteur bien que, pour plusieurs spécialistes, ils n'aient pas le même état d'esprit, voire le même niveau de compétence. Certains soutiennent également que les communautés d'OSINTers se rapprochent davantage de l'esprit des attaquants/hackers que du point de vue des défenseurs/experts SSI[281]. Victor Poucheret vient étayer l'idée d'une démarcation notable entre les spécialistes en défense et ceux de l'offensif. « *C'est un monde assez différent* » souligne-t-il, et de préciser de manière édifiante : « *mais qui devrait faire greffe pour une meilleure cohésion, et vis-à-vis notamment d'une dynamique patriotique*.[282] » Selon Pierre Penalba, fin connaisseur des deux mondes, les communautés de hackers ne sont pas celle des experts de cybersécurité classiques, les *blueteamers*, car les premiers pratiquent l'attaque et pensent invariablement « offensif ». Et d'ajouter : « *La communauté des hackers éthiques ce sont souvent des redteamers. On ne peut pas être les deux à la fois : blueteamer et redteamer, à la fois attaquant et défenseur. Et même si on n'est pas black hat, on va acheter des outils criminels pour les étudier (rétro-ingénierie) et les maitriser. Exemple : le malware Zeus, un cheval de Troie. Zeus, à l'origine, est développé par des hackers biélorusses, il a été diffusé, modifié/upgradé par des Russes pour en faire un outil encore plus puissant. On ne peut pas être un bon hacker éthique si on ne se frotte pas à ces outils.*[283] » Des propos corroborés par Jean-François Loewenthal, directeur la société Intelligences et chercheur associé au CF2R : « *Les bons, en défense, doivent connaître les mêmes outils que ceux des attaquants*.[284] »

[280] Interview Victor Poucheret et Brice Augras, *Thinkerview*, *op. cit.*
[281] Entretiens avec Alexandre Oda et Victor Poucheret. Nous traiterons d'OSINT en partie 3.
[282] Entretien avec l'auteur, 14/11/2021.
[283] Entretien avec l'auteur, 07/07/2023.
[284] Entretien avec Jean-François Loewenthal, 26/06/2017.

### c) *Le hacking est-il soluble dans le cadre légal et étatique ?*

L'état d'esprit des hackers est définitivement porté sur l'attaque et, on l'a dit, ces derniers tout comme les autorités ont d'une certain manière apprivoisé le concept d'éthique mais au regard de la légalité. Les premiers pour trouver une place dans un cadre jusqu'ici bien trop étroit, les secondes pour précisément encadrer des profils qui leur échappaient, dans le sens où elles ne les comprenaient et ne les contrôlaient pas. Du reste, si l'on s'en tient à l'éthique des hackers définie et théorisée par Steven Levy, l'expression de « hacking éthique » en est très éloignée. « *On a le même environnement technique*, explique Jean-François Loewenthal, […] *on a les mêmes techniques. La frontière n'est pas technique. C'est la frontière juridique qui change. Il y a donc une convergence par les "tuyaux".*[285] » Christian Harbulot, fondateur de l'École de guerre économique, abonde dans ce sens et parle d'une convergence seulement technique qui se fait par « *le contenant* », de communautés de pratiques réunissant autorités étatiques et hackers[286]. De surcroît et de manière éclairante, Jean-François Loewenthal précise que tout est conditionné au choix étatique et à celui des individus. En d'autres termes, l'État peut emprunter aux hackers leur état d'esprit offensif et leur offrir un cadre plus souple, tandis que les hackers peuvent se conformer davantage au moule du droit.

### d) *Une greffe peut-elle s'opérer entre les hackers et les autorités ?*

« La France, combien de divisions ? » pourrait-on s'interroger. Autrement dit, si des moyens y compris offensifs sont alloués à la cyberdéfense, en est-il de même pour la sécurité numérique, entendue comme l'ensemble du spectre de l'espace matriciel national ? Le pays peut-il compter sur une stratégie globale intégrant notamment ces profils très spéciaux que sont les hackers ? Quelle charnière établir avec ces acteurs certes atypiques mais sans doute incontournables ?

Prenons ce message de Victor Poucheret à l'adresse de sa génération :

> « *Comprendre d'où ça vient. le monde évolue vite, les technologies évoluent vite, les effets de mode évoluent vite, et quand on est jeune on est dans une bulle, et cette bulle-là elle est constituée de nos interactions sociales. Ces interactions sociales-là, malheureusement et heureusement, définissent une partie de notre personnalité, la manière dont on va évoluer. Ces interactions sociales sont aujourd'hui beaucoup modulées par la tech, par les réseaux sociaux, par les tendances que l'on peut voir passer maintenant, sur l'outil qu'est Internet. Et, pour moi, il faut être capable à un moment de dire stop, de déconnecter et de se dire bon : pourquoi c'est comme ça ?*

[285] Entretien avec l'auteur, 26/06/2017.
[286] Entretien avec l'auteur, 22/08/17.

*Pourquoi ça va dans ce sens-là, à qui profite le crime, où va l'argent et, derrière, vous pouvez très bien dire : j'ai envie de me former. Comment ça marche, d'où ça vient ?* [287]»

* * *

En définitive, les hackers ne sont-ils pas des garants de l'esprit critique ? Ne forment-ils pas des sentinelles tel un système immunitaire du monde numérique ? Derrière la supposée prise en compte par les autorités françaises de ces profils atypiques, qu'en est-il réellement ? La France a-t-elle, en lien avec ces hackers, posé les bases d'une véritable *cybersécurité offensive intégrée* ? Pour en juger, il nous faut analyser le niveau d'interaction entre ces acteurs. Notre instrument de mesure prendra la forme d'une grille d'analyse fondée sur les caractéristiques-clés de l'intelligence économique, qui vont nous permettre de sonder les rapports qu'entretiennent les institutions publiques et privées avec les hackers.

[287] Interview de Victor Poucheret, *Thinkerview*, *op. cit.* Il a 24 ans à l'époque de l'émission (2021).

# II. L’intelligence économique comme grille de lecture

# Chapitre 3 | Le postulat d'une guerre économique

« *L'Humanité n'a aucune raison d'être soulagée, car nous n'avons rien fait d'autre que remplacer autant que possible la guerre sanglante par la guerre non sanglante*. »

Qiao Liang & Wang Xiangsui

« Si vous voulez la paix, faites la guerre économique ! » Voilà qui pourrait résumer la thèse de Bernard Ésambert, ingénieur polytechnicien et ancien conseiller de Georges Pompidou. Lorsqu'en 1971, il introduit le concept de « guerre économique », qu'il développera principalement dans deux ouvrages[288], Bernard Ésambert s'inscrit dans le sillage de Montesquieu et sa théorie du « *doux commerce* » pacifiant les relations internationales (RI*). Cette tradition libérale classique postule que la concurrence économique est source de paix, que la guerre est contre-productive, immorale et qu'elle ne fait qu'affaiblir les économies d'États œuvrant depuis 1945 à bâtir un système institutionnel censé canaliser la violence internationale. Toutefois, là où on penserait que Bernard Ésambert cautionnait le jeu d'une supposée *main invisible* du marché, celui-ci prônait en réalité un engagement complet de l'État et son pilotage d'une politique industrielle dans le cadre de la solidarité européenne. Expliquant déjà à l'époque que si le match (vite tranché par la diplomatie coercitive américaine) entre le marteau japonais et l'enclume états-unienne menaçait de marginaliser l'Europe, c'est la Chine qui reprendrait le rôle du premier avec le même résultat pour le Vieux continent.

Si l'éclairage et la réflexion de Bernard Ésambert ont eu le mérite de poser les termes du débat, c'est toutefois avec Christian Harbulot que le concept de guerre économique va prendre une ampleur inédite. Ancien militant rompu aux doctrines communistes de guerre de l'information, Christian Harbulot deviendra conseiller scientifique et politique, et principal contributeur au célèbre rapport Martre de 1994 sur l'intelligence économique et la stratégie des entreprises. C'est surtout au sein de l'École de guerre économique (EGE), co-fondée en 1997 avec le général Jean Pichot-Duclos, qu'il va développer et asseoir une nouvelle grille de lecture des relations internationales[289]. Sa thèse : **la poursuite de la puissance et les rapports interétatiques ont pris un tour nouveau depuis la fin de la guerre froide ; dans un environnement *a priori* pacifié, les États n'ont en réalité pas mis fin à leurs différends et compétition, et se livrent désormais à des conflits d'ordre**

[288] Bernard Ésambert, *Le Troisième Conflit mondial*, Plon, 1977, 346 p. ; *La Guerre économique mondiale*, Olivier Orban, 1991, 334 p.

[289] Lire à ce sujet Giuseppe Gagliano, *Guerre et intelligence économique dans la pensée de Christian Harbulot*, VA, 2016, 112 p.

**économique**. En parallèle et dans une même idée, le stratégiste-économiste américain Edward Luttwak invente le concept de *géoéconomie* et tisse la métaphore entre le monde économique et la sphère militaire[290]. Pensé comme un État-stratège, l'appareil gouvernemental se doit de piloter des politiques économiques dont les entreprises nationales sont le bras armé en vue d'investir, conquérir et dominer les nouveaux territoires fluides que façonne le marché planétaire. Néanmoins, ce nouveau paradigme va en France avoir maille à partir.

[290] Edward Luttwak, "From Geopolitics to Geo-economics. Logics of Conflict, Grammar of Commerce", *The National Interest*, été 1990, pp. 17–23 ; « L'arsenal de la géo-économie », *Revue des deux mondes*, avril 1995, pp. 119-128.

## **A.** *Un concept controversé et hétérodoxe*

*« On veut la liberté aussi longtemps qu'on n'a pas la puissance ;*
*mais si on a la puissance, on veut la suprématie. »*

Friedrich Nietzsche

Les notions de *globalisation* et *mondialisation*, avant disjointes, se sont entremêlées et on ne fait plus guère aujourd'hui la différence. D'un côté, la première est très largement liée à la doctrine libérale et prône la planétisation du marché en privilégiant les aspects financiers et commerciaux des échanges ; de l'autre, la mondialisation s'axe d'abord sur une réflexion mettant en avant les dimensions humaine et sociale du phénomène de rapprochement et mélange des territoires et des peuples. Dans le processus en cours ou plutôt son accélération et phase actuelle – celle des technologies de l'information-communication –, les deux approches se combinent et se nourrissent réciproquement sans toutefois résoudre le dilemme originel. Il n'est que d'observer le rendez-vous annuel du forum de Davos pour s'en apercevoir, qui cristallise le clivage entre l'approche économiste représentée par les pays riches doublés des grandes entreprises et l'approche sociétale portée par le mouvement altermondialiste. Sans remettre nullement en question cette donnée, la conjoncture actuelle demeure toutefois fondée sur un système capitaliste libéral qui prend racine dans les accords de Bretton-Woods en 1944 sous l'égide des États-Unis.

Dans un tel système, que même la conscience écologique critique n'a pas bouleversé, une question demeure : qui dominera le monde ? À cet égard, le courant réaliste des Relations internationales postule qu'en dépit de toute leur volonté dans l'Histoire à sceller des coopérations et à régler leurs conflits, les hommes sont nécessairement voués à ne pouvoir dépasser leur nature belliqueuse fondée sur un ordre mélien[291]. À l'heure où l'OMC semble impuissante comme jamais du fait même de son principal contributeur, le multilatéralisme semble marquer le pas[292]. Pourtant, sans exclure la dureté des rapports concurrentiels au sein des échanges internationaux, la grande majorité des économistes ou des universitaires, voire des spécialistes du militaire sont rétifs à l'idée d'une violence s'exerçant dans la sphère

[291] L'ordre mélien repose sur le *Dialogue mélien* exposé par l'historien grec Thucydide dans sa *Guerre du Péloponnèse*. Ce récit porte sur le débat posé par la petite cité insulaire de Mélos, qui ne souhaite prendre parti lorsqu'un des principaux belligérants, Athènes, lui enjoint de se positionner vis-à-vis de son rival spartiate. Mélos invoque alors la neutralité et s'attend à ce que le fort ne s'attaque pas au faible. Or, dans une logique toute nietzschéenne, Athènes écrase Mélos sans pitié en avançant que la morale n'a pas sa place et qu'en somme la loi du plus fort prévaut toujours.

[292] Depuis le mandat de Donald Trump et à ce jour, les États-Unis bloquent la nomination des juges de l'organe d'appel (OA) de l'ORD, l'Organe de règlement des différends qui, comme son nom l'indique, règle les litiges internationaux d'ordre commercial. Le fonctionnement de l'OMC s'en voit fortement dégradé.

économique. Certes, la concurrence acharnée des entreprises privées peut crisper les relations internationales, mais la violence reste perçue comme l'apanage des acteurs politico-militaires et, surtout, cette compétition n'engendre aucun mort. Au pire, c'est d'un processus de « destruction créatrice » schumpétérien qu'il s'agit, sorte de darwinisme économique « *soft* » permettant l'émergence sélective « naturelle » d'entreprises compétitives à travers une saine concurrence. Quant à bon nombre d'experts des questions de défense, la violence est par définition cinétique et sanglante, et la simple adjonction de l'épithète « économique » au mot « guerre » n'aurait pas de sens. Pour ceux-là, l'économie est d'ailleurs l'inverse de la guerre puisqu'elle vise la création et non la destruction[293]. C'est toutefois oublier la face sombre du capitalisme et sa dimension éminemment politique.

### **1)** Nouvelles modalités des rapports de puissance

Fondée traditionnellement sur les capacités militaires des États, la puissance change de nature après 1991 avec la fin d'un ordre international jusqu'alors bipolaire. Des conflits plus indirects se substituent aux classiques affrontements armés reposant sur la coercition physique et la puissance de feu. Par ailleurs, la pacification ambiante et la sensibilité publique des sociétés occidentales au sortir d'un siècle de guerres vont confirmer le rejet de la conflictualité. À l'époque, certains analystes s'interrogent même sur la « volonté d'impuissance[294] » des pays riches, dont les populations aspireraient seulement à un confort matériel et le maintien d'un niveau de vie maximal. C'est que la puissance s'exerce désormais de manière plus subtile et notamment via l'influence, qualifiée par Joseph S. Nye de « *soft power* ». Le facteur économique, quant à lui, est à la croisée des voies de la puissance : entre *hard et soft power*[295]*,* emprise sur les choses matérielles et contrôle des esprits[296]. Ainsi, la guerre économique est fille de la globalisation. On assiste dès lors à « *l'avènement d'un nouvel ordre international où*

[293] C'est par exemple dès les années 1990 la position de Thierry de Montbrial, président de l'IFRI, vis-à-vis de la thèse de Bernard Ésambert qui, comme on l'a vu, n'est pourtant pas la plus radicale. Voir « La guerre économique mondiale, critique de Thierry de Montbrial », *Revue des deux mondes*, février 1992, pp. 125-132. Pour sa part, l'économiste libéral Élie Cohen, *La tentation hexagonale. La souveraineté à l'épreuve de la mondialisation*, Fayard, 1996, 453 p., assimilera la géoéconomie d'Edward Luttwak à un néomercantilisme.
Bien que le débat aujourd'hui soit plus nuancé, beaucoup de spécialistes du militaire expriment toujours un certain malaise autour de ce mariage « contre-nature » entre guerre et économie.

[294] Pascal Boniface, *La volonté d'impuissance. La fin des ambitions internationales et stratégiques ?,* Seuil, 1996, 208 p.

[295] On parle parfois de *smart power* pour désigner l'usage maîtrisé et conjoint des deux autres notions. Inventé là aussi par Joseph Nye, c'est Hillary Clinton qui popularisera le concept quand elle sera aux Affaires étrangères sous le mandat de Barack Obama.

[296] Le commerce, surtout, repose en grande partie sur des aspects immatériels liés à la publicité, au marketing et à la communication.

*l'arme économique remplacerait l'arme militaire comme instrument au service des États dans leur volonté de puissance et d'affirmation sur la scène internationale.*[297] »

Pour paraphraser Clausewitz, la guerre économique est la continuation de la guerre, et l'économie la poursuite de la politique par d'autres moyens. En d'autres termes, les États accumulent de la puissance par l'économie, et cette croissance est mise au service de leur intérêt national en vue d'acquérir puis conserver une suprématie stratégique mondiale. De fait, cette course à la puissance par des voies moins militaires et plus indirectes, via la maîtrise du triptyque *commerce-finance-monnaie*, débouche sur une dissymétrie de compétitivité et *in fine* la déstabilisation de l'équilibre international. Dès lors, les États vont user de stratagèmes pour tirer leur épingle du jeu en s'appuyant sur des doctrines politico-économiques. Naguère c'était le mercantilisme, aujourd'hui le néolibéralisme car toute dérégulation économique est en fait une régulation politique. Au-delà des *avantages comparatif* et *absolu* de David Ricardo et Adam Smith, le différentiel de compétitivité s'explique par une distorsion de la concurrence engendrée par des pratiques au mieux déloyales, au pire illégales. Pratiquée à divers degrés par tous les États, l'une de ces mesures minimales est le protectionnisme, pourtant caractéristique du mercantilisme. Faussant la concurrence aux yeux du pays qui le subit et la détournant à l'inverse pour celui qui le pratique, le protectionnisme est la face visible – mais souvent opaque[298] – du rapport de force engagé par les États en termes d'économie. En réalité cela va plus loin, puisque des manœuvres qui confinent à l'illégalité sont couramment employées : espionnage et pillage technologiques, diplomatie coercitive et mesures de rétorsion, extraterritorialité du droit (*lawfare*)… **En somme, l'économie est une guerre irrégulière parée des habits du conflit régulier**.

Cette mise en relation entre économie et politique est relativement récente dans l'Histoire. Au début du XVII[e] siècle, l'économiste français Antoine de Montchrestien est l'un des premiers à utiliser l'expression « d'économie politique » dans son *Traicté de l'oeconomie politique*[299]. Le vocable « économie » sera du reste séparé de son épithète seulement deux siècles plus tard avec l'avènement de la science économique. Dans les années 1970 et sous l'impulsion des sciences sociales anglo-américaines, l'économie politique internationale (EPI) va se définir très largement comme l'ensemble des rapports mutuels entre l'économique et le politique, le national et l'international. Et plus précisément, comme « *l'interaction réciproque et dynamique dans les relations internationales entre l'accumulation de la richesse et la*

[297] Pascal Lorot, « De la géopolitique à la géoéconomie », *Géoéconomie*, 2009/3 (n° 50), pp. 9-19, §4, citant Edward Luttwak, "From Geopolitics to Geo-economics…, *op. cit.*

[298] Le large spectre du protectionnisme va des plus évidents tarifs douaniers et quotas aux moins flagrantes normes réglementaires ; administratives ; sanitaires ; techniques et environnementales. Citons encore le contrôle des changes ou les subventions aux exportations…

[299] Antoine de Montchrestien, *Traicté de l'oeconomie politique : dédié en 1615 au Roy et à la Reyne mère du Roy (Éd.1889)*, Hachette-BNF, 2012, 520 p.

*poursuite de la puissance*[300]. » Il est intéressant de noter que ce sous-champ de la science politique – ou l'inverse selon ses tenants – cherche, d'une part, à répondre à la problématique de « l'interdépendance complexe » et, d'autre part, va apparaître dans le contexte intellectuel du débat décliniste américain. Face à cette perception fondée ou imaginaire, les sphères dirigeantes et universitaires états-uniennes cherchent à donner une orientation plus appliquée et prescriptive à la recherche académique pour répondre aux crises de la deuxième moitié du XXe siècle. On le voit, comme la géopolitique allemande en son temps, l'EPI américaine se veut une science-instrument de la puissance.

Cette réflexion sur l'articulation de l'économique et du politique va précisément ouvrir la voie au rapprochement avec les questions géopolitiques et, par-là, à la nouvelle discipline que constitue la géoéconomie dans le contexte post-guerre froide.

### **2)** Territoires et réseaux dans la globalisation : la géoéconomie

Définie comme « *L'étude des rivalités de pouvoir(s) et d'influence(s) sur des territoires* » par Yves Lacoste[301], la géopolitique consacre le postulat d'un conditionnement géographique des politiques d'État. Autrement dit, comme le dit la formule – possiblement apocryphe – de Napoléon Bonaparte : « *Un État fait la politique de sa géographie.* » C'est avant tout une méthode d'analyse basée sur le triptyque *intentionnalité politique–temps long–inscription territoriale.* On a beaucoup glosé sur la fin supposée de la géopolitique en tant que discipline pertinente pour expliquer les rapports de puissance. C'est largement dû à l'influence états-unienne et à sa science politique internationaliste pour laquelle la géopolitique notamment française n'a jamais été jugée crédible. On trouvera ainsi peu de géopolitologues américains contemporains, à quelques exceptions près mais déjà anciennes comme Nicholas Spykman ou le géostratège Alfred Mahan. Il faut dire que les *World Studies* tout comme l'*International Political Economy* sont des disciplines largement partisanes. C'est probablement pour cette raison que les tenants hexagonaux de la géoéconomie ont repris à leur compte le concept inventé, certes de l'autre côté de l'Atlantique, par un contradicteur de Francis Fukuyama[302]

[300] Selon Robert Gilpin, *The Political Economy of International Relations*, Princeton University Press, 1987, 472 p., traduit dans Stéphane Paquin, *Économie politique internationale*, Paris, Montchrestien, 2009, 160 p.

[301] Grand spécialiste français et international de la discipline. Parmi ses œuvres principales on compte Yves Lacoste, *La géographie, ça sert, d'abord, à faire la guerre*, La Découverte Poche, 2014, 248 p. et *Dictionnaire de géopolitique*, Flammarion, 1996, 1728 p.

[302] Son postulat de « *la fin de l'Histoire* » est bien connu. Dans un ouvrage éponyme et au sortir de la guerre froide, sa thèse revient à dire que l'Occident a triomphé face au communisme et que le monde entier va se convertir à la démocratie libérale de marché. De ce fait, il n'y aura plus de conflit, c'est la fin de la guerre, donc la fin de l'Histoire. Cette formule est traditionnelle chez les historiens, la guerre étant perçue comme accélérateur et facteur fondamental de la projection de l'Humanité dans le temps et l'espace. Voir Francis Fukuyama, *La fin de l'histoire et le dernier homme*, Flammarion, 1992, 456 p.

(Edward Luttwak) pour asseoir son discours dans une France déjà passablement aveuglée par la vision américaine de la mondialisation. Ainsi que nous le montre le conflit russo-ukrainien engagé depuis février 2022, la géopolitique est loin d'avoir dit son dernier mot. Mais les empires étant désormais plus immatériels, c'est sur son socle que va se développer l'angle d'analyse géoéconomique.

Héritier politiste français d'Edward Luttwak, Pascal Lorot définit la géoéconomie comme « *l'étude des stratégies économiques et commerciales soutenues par les États pour protéger leur économie nationale, notamment certains segments stratégiques et certains fleurons nationaux, maîtriser de nouvelles technologies-clés et conquérir de nouveaux marchés, le tout dans un même objectif de puissance et d'influence globale que d'un point de vue géopolitique, mais dans le domaine économique et commercial.* […] *Elle s'interroge sur les relations entre puissance et espace, mais un espace « virtuel » ou fluidifié, au sens où ses limites bougent sans cesse, donc un espace affranchi des frontières territoriales physiques caractéristiques de la géopolitique*.[303] »

À cet égard, nous pensons qu'il faut dépasser le clivage stérile qui demeure entre la géopolitique, fille de l'État-nation, et la géoéconomie, fille de la mondialisation. L'architecture internationale est aujourd'hui fondée sur le croisement entre le territoire (physique, vertical, national) et le réseau (plus immatériel, horizontal, transnational). Au territoire classique, l'inertie et la permanence ; au réseau, le changement perpétuel et l'instabilité chronique. Les deux disciplines ne peuvent donc s'exclure l'une l'autre mais se combinent au contraire pour disposer des lunettes les plus adaptées pour voir le monde. Les héritages de l'industrialisation et de la croissance sont aujourd'hui ébranlés : c'est le retour d'une certaine manière à la dialectique entre sédentarité (le territoire) et nomadisme (le réseau). La phase actuelle de la globalisation implique non un changement brutal du monde, mais un mouvement permanent qui exige des États de défendre et attaquer simultanément. Ancré sur son territoire, l'État doit rendre celui-ci attractif d'une part, et se projeter vers l'extérieur d'autre part. D'où sa schizophrénie : tenu à la fois d'ouvrir et fermer ses frontières, conserver son identité mais être perméable à la prolifération des idées, protéger ses innovations techn(olog)iques mais accueillir celles des autres[304]… Puissance et influence se conjuguent donc, et si l'effet de loupe induit par le traitement médiatique du conflit ukrainien nous ramène à nos études – de géopolitique –, c'est bien la capacité d'influence et les intérêts économiques des États qui prévalent sur l'intérêt politique pur et la puissance dure. Du reste, la définition aujourd'hui

[303] Pascal Lorot, *Introduction à la géoéconomie*, Economica, 1999, 244 p., p. 15.
[304] Philippe Moreau-Defarges, *Introduction à la géopolitique*, Seuil, 2009, 272 p.

communément admise de la puissance comporte un volet de *soft power* mettant en exergue la capacité à faire adhérer au modèle forgé par un État le plus grand nombre d'acteurs[305].

Revenons dès lors à la définition de Pascal Lorot. La globalisation a ainsi propulsé sur le devant de la scène des organisations multi- puis trans-nationales animées par des objectifs et stratégies planétaires. Ainsi, l'espace « fluidifié » qu'elle concourent à tisser, c'est le réseau ou plutôt les réseaux de toutes natures, germes et fruits de flux informationnels, humains, idéologiques et culturels, économiques et financiers, lesquels façonnent des territoires horizontaux en quelque sorte virtuels. Or, les États ne sont jamais bien loin, et si certaines entreprises semblent parfois vouloir s'émanciper de cette tutelle (GAMAM/États-Unis notamment) et servent toujours leur propre agenda, il n'en demeure pas moins que les unités politiques sont à la manœuvre et les intérêts réciproques et cohésifs de chacun bien sentis[306]. À cet égard, les exemples notamment états-unien, israélien, suédois, chinois ou japonais sont très significatifs. Aussi, « *quand l'État intervient, lorsqu'il encourage, assiste ou dirige ces mêmes activités* [investir, chercher, développer et trouver un marché…], *ce n'est plus de l'économie "pur sucre", mais de la géoéconomie.*[307] »

Chez Pascal Lorot, là s'arrête toutefois l'emprunt au positionnement résolument guerrier du stratégiste américain, dans une vision plus édulcorée. Alors, a-t-il raison d'indiquer que la perception d'un « *libre-échange poussé dans ses retranchements les plus ultimes par une concurrence planétaire chaque jour davantage exacerbée* […] *comme étant désormais un jeu à somme nulle, où gagner une part de marché revient, de fait, à éliminer son adversaire*. », cette perception donc est-elle, seulement « […] *peut-être plus forte que la réalité elle-même* »[308] ? Le politiste-économiste français ne s'en cache pas : la vision offensive d'un Luttwak invoquant trois principales armes économiques : la R&D (« *artillerie* »), l'appareil productif (« *infanterie* ») et la prédation financière (« opérations commando » ?), le dérange. La géoéconomie selon lui ne peut céder le pas à l'approche martiale, laquelle admettrait à tout prendre des « *politiques* (sic) *de guerre économique* » menées en réalité par des acteurs non gouvernementaux. Car, pour leur part, les États ne mèneraient que des « *politiques*

[305] Voir par exemple Gérard Dorel, https://geoconfluences.ens-lyon.fr/glossaire/puissance (consulté le 25 juin 2023), qui met l'accent sur le poids et l'influence économiques et culturelle des États. Raymond Aron la définissait comme la capacité à influencer les autres sans être trop influencé en retour.

[306] Comme le confirme Philippe Truillet, entretien du 15/09/2017, « *il y a eu souvent collusion entre l'État américain et les GAMAM. C'est une question de puissance et de surveillance dans le cyberespace.* » Par ailleurs, on peut noter que les organisations ou accords d'intégration régionale (Mercosur, ALENA, ASEAN, UEEA, UE…) ne sont que l'expression d'une forme de coopétition régie par des rapports de force interétatiques. Ce qui permet d'avancer que la mondialisation se cristallise en réalité par une régionalisation de blocs hétérogènes, eux-mêmes en concurrence.

[307] Edward Luttwak, *Le rêve américain en danger*, Odile Jacob, 1995, 462 p., p. 34.

[308] Pascal Lorot & François Thual, « La géoéconomie, nouvelle grammaire des rivalités internationales », *Introduction à la géopolitique*, Montchrestien, 158 p., pp. 122-123.

*concurrentielles offensives acceptables par la communauté internationale, parce qu'affranchies des pratiques économiques les plus agressives et masquées que l'on retrouve dans ce que l'on appelle "guerre économique*".[309] » En d'autres termes, les dérives potentielles de l'économie ne la résument pas.

Cette position traduit-elle comme un réflexe conditionné de la part des analystes hexagonaux, à l'instar des élites politiques françaises ? Là est peut-être le paradoxe alors qu'il est question d'activités qualifiées de politiques proprement « offensives ». Où se situe ainsi le curseur quand par exemple le droit, domaine littéralement légitime, est instrumentalisé à des fins politico-économiques dans l'arène mondiale ? Il y a, à notre sens, un problème de définition intrinsèque à l'interrogation de Pascal Lorot : la guerre économique s'assimile-t-elle, est-elle un succédané à la géoéconomie[310] ? La question n'est pas posée dans les bons termes : considérer qu'il s'agit d'une simple alternative sémantique, c'est dès lors nier la différence de nature entre les deux notions. Or, s'il existe des dispositifs géoéconomiques, c'est bien la démonstration d'une prise en compte de la dimension *a minima* belligène de l'économie. En effet, quand la guerre économique est en réalité le décor contextuel de la conflictualité ambiante, la géoéconomie de son côté forme une solution, un moyen pour faire cette guerre ou du moins y répondre. Au pire est-ce une différence de degré, que marque résolument l'école de pensée française sur la guerre économique.

### **3)** Une école de pensée sur la guerre économique, une école française de l'IE

> « *La France ne le sait pas, mais nous sommes en guerre avec l'Amérique. Oui, une guerre permanente, une guerre vitale, une guerre économique, une guerre sans mort apparemment. Oui, ils sont très durs les Américains, ils sont voraces, ils veulent un pouvoir sans partage sur le monde. C'est une guerre inconnue, une guerre permanente, sans mort apparemment et pourtant une guerre à mort.*[311] »
>
> François Mitterrand

Contrairement à ce qu'a professé Francis Fukuyama en 1992[312], l'Histoire n'a pas vu sa fin arriver. Or, la fin de celle-ci signifiait la fin de la guerre et l'homogénéisation d'un monde pacifié sous le régime de la démocratie libérale de marché. Cette *pax americana* n'est pas advenue, pas plus que la « mondialisation heureuse » célébrée par l'essayiste Alain Minc. La guerre traditionnelle est loin d'avoir disparu et, en outre, l'épisode ukrainien ne doit pas masquer la longue série de conflits armés qui émaillent l'histoire immédiate sur presque tous

[309] Pascal Lorot, « De la géopolitique à la géoéconomie », *op. cit.*, §14-20.
[310] Pascal Lorot, *Ibid.*, §15.
[311] Georges-Marc Benamou, *Le dernier Mitterrand*, Plon, 1996, 264 p., p 52.
[312] Francis Fukuyama*, La fin de l'histoire...*, *op. cit.*

les continents. Quant à la nature économique de la conflictualité, elle va s'exprimer de manière éclatante lorsque les États-Unis de Bill Clinton vont ni plus ni moins déclarer la guerre économique au reste du monde. Il y a bien un malentendu dans l'air, comme le signifie en substance Nicolas Moinet : l'économie n'est pas une compétition loyale entre *gentlemen* pour vendre le meilleur produit au meilleur prix dans un monde de libre concurrence. Il faut donc démasquer l'économie et se rendre à l'évidence : « […] *la guerre économique n'est pas* une perversion du système, mais bien LE système, […] *l'expression de rapports de force et d'intérêts de puissance*.[313] » C'est ce que s'attache à faire depuis vingt ans la communauté française de l'intelligence économique.

« *Nous ouvrirons les marchés étrangers avec une barre à mine où cela est nécessaire, mais avec une poignée de main toutes les fois où cela est possible*.[314] » Le ton est donné en 1989 par la représentante au commerce de G.H. Bush, Carla Hills. Cette prise de conscience d'un long fil d'Ariane historique de la conflictualité économique, on la doit principalement à Christian Harbulot qui, fin des années 1980, mène des travaux pour le compte du gouvernement, lesquels aboutiront à un état des lieux intitulé *Techniques offensives et guerre économique*[315]. Malgré les travaux pionniers pourtant anciens de François Perroux[316] ou de l'historien Fernand Braudel, cette réflexion n'a alors pas été élaborée en France. D'après Christian Harbulot, ce sont les travaux de Georges-Henri Soutou qui, sur cette base, vont esquisser une analyse de la guerre économique[317]. Pour cause, la guerre froide a oblitéré les conflits internes au bloc de l'Ouest déjà affairé à lutter contre son homologue à l'Est ; il s'agissait, en effet, de ne prêter aucun flanc aux tentatives de déstabilisation provenant du camp adverse.

Ainsi, plusieurs raisons diachroniques président à cette cécité du monde académique mais aussi de la sphère politique. De l'ère coloniale et son commerce triangulaire aux motifs larvés des deux guerres mondiales en passant par la justification morale des Croisades médiévales, l'interprétation politico-militaire a toujours pris le pas sur les implications économiques des logiques de domination. Plus généralement et récemment, un courant libéral néoclassique s'est imposé qui élude la place de la politique et des relations de puissance dans l'économie ; inconsciemment pour bon nombre d'élites européennes, et à dessein en revanche

[313] Nicolas Moinet, *Les sentiers de la guerre économique.* T1 – *L'école des nouveaux "espions"*, VA, 2018, 192 p., p. 12.

[314] Voir https://www.ege.fr/sites/ege.fr/files/downloads/CE_162_IEEE_Christian_Harbulot_FR.pdf ; https://www.finance.senate.gov/download/nomination-of-carla-anderson-hills&download=1.

[315] Christian Harbulot, *Techniques offensives et guerre économique*, La Bourdonnaye, 2014 (2e éd.), 159 p.

[316] Économiste du XXe siècle ayant produit une somme critique et étayée de la pensée libérale.

[317] Notamment dans Georges Henri Soutou, *Le sang et l'or. Les buts de guerre économiques des grandes puissances*, Fayard, 1990 ; et *La guerre froide*, Fayard, 2011, qui évoque la dimension économique de l'affrontement Ouest-Est.

de l'autre côté de l'Atlantique. Comme le mentionne Olivier de Maison Rouge[318], les Américains ont pris conscience en 1991 qu'il fallait modeler un nouvel ordre international fondé sur le droit d'un libre commerce acquis à leur cause. En fait de droit universel, il s'est agi d'imposer leur propre interprétation de la règle juridique, qui a accouché d'une doctrine interventionniste reposant sur une vision élargie de la sécurité nationale[319]. En 1993, en effet, l'administration Clinton crée un dispositif géoéconomique offensif[320], tandis que son secrétaire d'État, Warren Christopher, déclare publiquement que la « sécurité économique » doit être élevée au rang de suprême priorité de la politique étrangère. Dans une perspective tout américaine, chacun a ses chances dans cette compétition tenue pour un jeu à somme positive. Dans la réalité, le narratif cache maladroitement la promotion de l'intérêt national états-unien, « *mêlant finalement une rhétorique à la fois libérale et mercantiliste, des principes peu compatibles aux yeux d'économistes mais parfaitement légitimes pour les politiques*.[321] » Inspiré du Japon technoglobaliste des années 1980, ce dispositif, voire cette « machine de guerre économique »[322], a depuis lors été abondamment décrit et caractérisé : synergie des partenariats public-privé ; orientation économique des agences de renseignement ; instauration d'un « protectionnisme éducateur[323] » sélectif ; façonnement normatif de portée mondiale ; arsenalisation du droit articulée avec un système d'injonctions morales et des vecteurs d'influence culturelle et commerciale…

S'il a fallu deux décennies pour que la réflexion sur cette dimension conflictuelle voit le jour et nourrisse la littérature scientifique, le postulat d'une guerre de nature économique s'est peu à peu imposé au gré des ingérences étrangères subies par la France. Les cas de prédation économique caractérisée se compte désormais en grand nombre et défraient régulièrement la chronique. La politique peu subtile de Donald Trump a permis une certaine prise de conscience en Europe, même si les réflexes conditionnés sont tenaces. Plus qu'une hypothèse, la guerre économique est devenue une grille de lecture de la conflictualité contemporaine et des rapports

[318] « Penser la guerre économique », conférence tenue à SciencesPo Lyon, 29 novembre 2018.
[319] Sous la forme d'un *continuum* intérieur–extérieur et sécurité–défense (cette approche, bien que préfigurée par le Code pénal de 1994 comme nous le verrons plus loin, sera officialisée en France seulement avec le LBDSN 2008). À l'issue de plusieurs débats, la science politique américaine introduit une redéfinition de la sécurité nationale, fondée désormais sur une projection vers l'extérieur partout où les intérêts du pays peuvent être mis en cause.
[320] Notons la création par le vice-président Al Gore d'une *War Room* au sein du département du Commerce.
[321] Voir https://www.revueconflits.com/guerre-economique-histoire-mondialisation-entreprises-etats-frederic-munier/, consulté le 20 juin 2023.
[322] Christian Harbulot, *La machine de guerre économique*, Economica, 1992, 178 p.
[323] Le *protectionnisme éducateur* est un concept forgé par Friedrich List, l'inventeur du *Zollverein*, union douanière germanique qui a concouru à la création de l'État-nation allemand en 1971. Il consiste à protéger artificiellement (subventions publiques) un secteur ou une filière économique le temps de lui permettre de se mettre au niveau des meilleurs compétiteurs internationaux. Fin 2022, par exemple, Emmanuel Macron s'est rendu aux États-Unis au nom de l'UE pour prier Joe Biden de bien vouloir mettre fin à une telle pratique au sujet des industries des énergies renouvelables. Voir https://www.radiofrance.fr/franceculture/podcasts/l-esprit-public/emmanuel-macron-a-l-offensive-contre-le-protectionnisme-americain-3518508, consulté le 10 juin 2023.

de puissance. Fort de cette assise gagnée de haute lutte, le mouvement intellectuel qui l'a initiée a acquis ses lettres de noblesse. À l'âge de la maturité, ce dernier a pris la forme d'une *école de pensée sur la guerre économique* cofondée en 2018 par cinq de ses plus grands promoteurs et théoriciens : Chistian Harbulot, Nicolas Moinet, Ali Laïdi, Éric Delbecque et Olivier de Maison Rouge[324]. Comment peut-on alors définir cette conflictualité avec précision ?

La guerre économique est avant tout une guerre cognitive et informationnelle dont l'objectif dissimulé est de façonner l'esprit de son adversaire pour *in fine* le « vaincre sans combattre ». Plus flagrant en temps de guerre (blocus en tous genres, attrition et destruction physique des infrastructures et industries, ciblage de la logistique ennemie…), l'art de la guerre économique consiste désormais en une stratégie de domination indirecte en temps de paix. Si l'on emprunte au général Beaufre, « *la stratégie est l'art de la dialectique des volontés utilisant la force pour résoudre leur conflit*[325]. » Si l'on admet que l'économie est une composante du *hard power*, cette définition se révèle déjà pertinente. Toutefois, la caractéristique de la guerre économique est que cette dialectique est souvent inexistante, car nombre d'acteurs ne se considèrent tout simplement pas comme des belligérants et n'ont donc pas conscience d'être attaqués. C'est ce que Christian Harbulot appelle un « encerclement cognitif », dont le prédateur économique use pour envelopper ses proies dans un maillage de dépendances fortes (emprise financière, servitude technologique, obédience idéologique et formatage des esprits, assujettissement normatif et soumission juridique…[326]). Ainsi, c'est sur plusieurs *échiquiers invisibles* que jouent désormais les acteurs des relations internationales : États, entreprises, ONG, individus… le cycle guerre-paix n'est plus. De fait, la stratégie est devenue globale et l'outil militaire n'en est qu'un mode parmi d'autres dont l'usage n'est d'ailleurs globalement plus pensable en Occident. Pour Christian Harbulot, la mutation de la puissance est le point d'entrée, et elle donne lieu à une *guerre économique systémique*[327] fondée sur la capacité à dissimuler ses intentions et ses manœuvres d'influence. On soumet donc toujours l'adversaire à notre volonté mais, dans cet environnement conflictuel global, « *les coups portés sont principalement de nature informationnelle et leur identification est rendu indéchiffrable à cause de l'extrême complexité de la société de l'information.*[328] »

[324] https://www.epge.fr/

[325] André Beaufre, *Introduction à la stratégie*, Hachette Littératures, 1998 (2e éd.), 192 p., pp. 33-34.

[326] Éric Delbecque insiste : « *L'extra-territorialité du droit américain est peut-être l'une des armes les plus puissantes des États-Unis, et un symptôme notable de la guerre économique actuelle*. » (Conférence « Penser la guerre économique », SciencesPo Lyon, 29 novembre 2018)

[327] Christian Harbulot (entretien), « Chine/États-Unis ? Sortie de crise ?… La guerre économique systémique comme grille de décryptage » *Communication & Influence*, n°111, mai 2020.

[328] Christian Harbulot, *L'art de la guerre économique*. *Surveiller, analyser, protéger, influencer*, VA, 2018, 152 p., p. 36.

Au bilan et à défaut d'une définition encore fixée, nous reprenons celle d'Ali Laïdi selon qui :

> « *La guerre économique renvoie à l'utilisation par des acteurs étatiques ou privés de pratiques déloyales ou illégales dans leurs relations économiques, en temps de paix sans conflit ni diplomatie préalable, à la fois entre pays amis et ennemis*.[329] »

Pour y répondre, il faut ainsi changer de posture intellectuelle et penser tout autant que mener ces nouvelles formes de combat. Dérivée du constat et de cette prise de conscience, l'intelligence économique s'est ainsi structurée en art et science de cette guerre.

[329] Conférence « Penser la guerre économique », SciencesPo Lyon, 29 novembre 2018.

## **B.** *L'IE ou le pari d'une intelligence collective souveraine*

« *Faire la guerre sans l'aimer.* »

André Malraux

L'intelligence économique (IE) est devenue un champ (inter)disciplinaire placé principalement au carrefour des sciences de gestion et des sciences de l'information-communication[330]. Tout comme ces dernières, qui singulièrement imbriquent leurs deux composantes séparées ailleurs, l'intelligence économique est le fruit d'une école française spécifique qui s'est hissée au rang des approches les plus abouties et reconnues. Définie succinctement comme « *le processus de traitement de l'information stratégique*[331] » à vocation économique, l'IE s'est peu à peu intégrée au paysage institutionnel et entrepreneurial français dans le cadre d'une politique publique et comme méthode de management au sein de firmes privées. Concept protéiforme emprunté à la *competitive intelligence* (CI) américaine et introduit dans l'Hexagone par Robert Guillaumot[332], elle a fait l'objet de plusieurs législations parcellaires qui ont produit des résultats variables.

Cette spécificité de l'IE est d'autant plus intéressante que son équivalente anglosaxonne (CI) aborde la discipline du point de vue des organisations privées vers le monde politique en tant que leur coopération est pourvoyeuse d'avantages compétitifs. En France, l'institutionnalisation de la discipline revêt une dimension politique plus verticale puisque l'échelle envisagée est celle de l'économie d'un pays et a donc trait à la posture géoéconomique de l'État. Au global, l'IE en France peut s'appuyer sur trois pôles qui se nourrissent réciproquement : le monde de la recherche, celui de l'enseignement, et enfin la sphère entrepreneuriale. En vingt ans, cette synergie a produit des effets notables qui, cependant, buttent sur des difficultés principalement politiques et administratives. En effet, après les premiers succès d'estime sous l'influence de précurseurs universitaires, de législateurs mobilisés et d'initiatives territoriales (collectivités), l'IE se trouve régulièrement entravée dans son application, dénotant une sorte de bricolage situationnel au mieux tactique et sans vision de long terme. À l'image tocquevillienne d'un « génie et d'un mal » français, le pays serait victime d'une inconstance enracinée à appréhender un horizon stratégique. En somme, la

[330] Selon une étude de Christian Marcon *in* Alice Guilhon & Nicolas Moinet (dir.), *Intelligence économique. S'informer, se protéger, influencer*, Eyrolles, 2016, 352 p., p. 324, 75% des thèses de doctorat consacrées à l'IE étaient issus de ces deux disciplines entre 2000 et 2015.

[331] Alice Guilhon & Nicolas Moinet (dir.), *op. cit.*, p. 6.

[332] Créateur de nombreuses entreprises d'informatique logicielle, il a initié le mouvement de l'IE en France en tant que membre de l'association états-unienne SCIP (https://www.scip.org/), et fondé en 1993 l'Académie de l'intelligence économique.

France n'a pas opéré sa mue complète et après moult vicissitudes il lui faut encore relever plusieurs défis pour dissiper le brouillard de la guerre économique.

À défaut de s'être réellement érigée en État-stratège, elle a toutefois le potentiel de l'État-stratégiste. Après une description à grands traits de cette science de l'IE puis la caractérisation théorique et opérationnelle de la discipline, nous verrons que dans un monde globalisé et numérisé l'IE peut apporter, dans l'esprit comme dans la lettre, sa contribution à la cyber-conflictualité.

## 1) Une posture de combat, une philosophie de l'action : fondamentaux de l'intelligence économique

« *Les sociétés politiques ne sont pas ce qu'en font leurs lois*
*mais ce que les sentiments, les croyances, les habitudes du cœur*
*et l'esprit des hommes qui les ont formés les ont préparés à être.* »

Alexis de Tocqueville

### a) *Une notion floue dans un contexte de turbulences*

Si les États-Unis sont les précurseurs du concept d'*intelligence organisationnelle*[333] dès 1967, puis celui subséquent de *sécurité économique* au début des années 1990, la France n'est pourtant pas restée inerte. Ainsi, un premier pas indirect d'ordre législatif est réalisé en 1994 avec le renouvellement du Code pénal qui introduit la notion *d'intérêts fondamentaux de la nation*[334]. Il s'agit d'adapter l'appareillage juridique aux nouvelles menaces encore mal comprises que la mondialisation fait surgir. Un an auparavant, l'ancien directeur de la DGSE, l'amiral Pierre Lacoste, plaidait d'ailleurs pour la reformulation politico-opérationnelle de la *défense nationale* et son remplacement par le concept plus large et adapté de *sécurité nationale*[335]. En dépit de nombreuses controverses d'interprétation légaliste, rapporte Bertrand Warusfel, ce texte a été considéré unanimement comme une véritable révolution juridique, opérant un renversement doctrinal de la relation défense/sécurité. En somme, au même titre que la stratégie a longtemps représenté une sous-partie de la guerre laquelle s'est transformée – ou redevenue – en une sous-partie de la stratégie, la défense s'est subordonnée à la sécurité pour n'en devenir qu'un moyen. En propulsant le concept d'intérêts

[333] Harold Wilensky, *Organizational Intelligence Knowledge and Policy in Government and Industry*, Basic Books, 1967, 226 p. Citons par ailleurs les travaux fondateurs de Michael Porter. Le concept d'intelligence organisationnelle se déclinera à l'envi : *competitive/market/business intelligence…*

[334] https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006136044/

[335] Bertrand Warusfel, « Les notions de défense et de sécurité en droit français », *Droit & Défense*, n° 94/4, octobre 1994, pp. 11-20, p. 1.

fondamentaux, on a permis à de nouveaux domaines, tel celui de patrimoine scientifique et économique national, d'être considérés comme des actifs stratégiques – du moins en théorie[336]. Cette inertie du droit a en outre eu pour conséquence de générer de nouvelles notions, à l'instar de la *défense économique* aujourd'hui caduque.

### b) *Une définition aux contours incertains en dépit de constats clairs*

Le débat originel de l'intelligence économique a bien porté sur sa définition et même sa traduction non littérale (*competitive intelligence*) de l'anglais. C'est ce qui transparaît d'ailleurs de l'appellation du rapport dit « Martre », première étape-clé du travail législatif produit sur l'IE. Précisément intitulé « *Intelligence économique et stratégie des entreprises*[337] », ce dernier propose une première définition, déjà très complète, de la discipline et l'érige en pratique managériale à l'adresse des organisations privées dans une optique avant tout défensive. Il constitue l'acte fondateur de l'intelligence économique en France en faisant, d'une part, deux constats : celui des faiblesses (dispersion des efforts, mauvaise coordination globale, manque de communication et rapports hiérarchiques conflictuels, cloisonnements administratif et organisationnel) et le constat de freins cognitifs (faible conscience des enjeux de guerre économique, mécompréhension de l'IE perçue comme de l'espionnage ou assimilée à la seule veille technologique). D'autre part, le rapport élabore des préconisations fondées sur le manque de compétitivité générale des entreprises nationales[338] :

1. *Diffuser la pratique de l'intelligence économique dans l'entreprise* :

Responsabiliser les chefs d'entreprises, sensibiliser et inclure les personnels dans la mise en place d'un système d'IE ; faire un suivi et des retours d'expérience ; diffuser l'information utile.

2. *Optimiser les flux d'informations entre le secteur public et le secteur privé* :

Décloisonner et optimiser le partage d'informations économiques entre administrations, collectivités et entreprises (s'inspirer des sociétés de commerce allemandes ou japonaises – *sôgô shôsha*) ; pilotage et incitation étatiques à projets ; organisation en réseaux.

3. *Concevoir les banques de données en fonction des besoins de l'utilisateur* :

Reprise en main nationale de la provenance, de la gestion et du stockage des données (posant avant l'heure la question brûlante de la *souveraineté numérique*) ; nationalisation de la

[336] Olivier de Maison Rouge, Conférence « Penser la guerre économique », *op. cit.*, note que le concept de sécurité nationale n'est présent que dans un article du Code de la Défense, « *donc seulement sur le plan militaire. Il nous faut sortir du champ purement militaire, pour étendre la sécurité nationale au champ économique*. »

[337] Henri Martre, Philippe Clerc, Christian Harbulot, *Rapport du groupe « Intelligence économique et stratégie des entreprises »*, 1994, 167 p. (https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/rapport-martre.pdf). Ce rapport a été supervisé par Henri Martre, ingénieur, entrepreneur, et alors député, ainsi que Philippe Clerc, alors conseiller-expert au Commissariat général du plan, et actuel directeur de l'Académie de l'IE.

[338] Axes de préconisations finales du rapport Martre, *ibid.*, pp. 94-100.

production de bases de données en partenariat privé avec des cabinets ; assurer l'accès facilité à celles-ci.

4. *Mobiliser le monde de l'éducation et de la formation :*

Former des professionnels dans le cadre de formations universitaires spécifiques à l'IE pour alimenter les ressources humaines des entreprises ; créer des pôles de recherche et les connecter aux établissements éducatifs pour mobiliser leur intérêt à ces formations (écoles de commerce et de management, universités, grandes écoles…).

Comment définir préalablement l'IE ? Voici la proposition du rapport Martre :

« *L'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût.*[339] »

Même si l'on retient communément cette définition, le texte explicite plus largement – et peut-être cela brouille-t-il le message – les tenants et aboutissants de l'objet « IE ». Par exemple, on ne retient guère ici l'aspect offensif de la discipline, pourtant déjà présent dans ce rapport.

### c) *Un objet complexe dans un monde complexifié*

En dépit de son ambiguïté intrinsèque, le rapport Martre va consacrer l'expression « intelligence économique ». Quel sens alors retenir du mot « intelligence » : son acception polysémique anglosaxonne ou sa définition étroite française ? En réalité, il faut chercher dans le croisement des deux : renseignement et capacité cognitive. Le terme *intelligence* renvoie bien sûr à la culture et au système anglosaxons du renseignement (*intelligence services)* qui, croisé avec la terminologie française confère à la capacité de relier des éléments disparates et diffus en vue de leur intelligibilité : « *lire entre les lignes* (*en latin* inter-legere)*, comprendre (le dessous des cartes) en recueillant et en assemblant (en grec* lego*) mais aussi surprendre (l'intelligence rusée de la déesse* Mètis*)* » selon les mots de Nicolas Moinet. En somme, dans un monde complexe où la logique de réseau prévaut, il faut adapter avec acuité son appréhension de la réalité. Au renseignement la culture et la méthode, à l'intelligence l'exploitation et l'action d'influence.

### d) *Une culture et une méthodologie du renseignement*

Renseigner, c'est ré-enseigner, ainsi enseigner de nouveau. C'est bien la philosophie du renseignement, qui consiste en l'axiome socratique *savoir qu'on ne se sait rien*, ou de manière

[339] Rapport Martre, *op. cit.*, p. 11.

plus pragmatique à s'instruire en pensant contre soi-même. L'objectif est de s'approprier les outils et méthodes des services de renseignement, à commencer par le cycle de management de l'information adopté très largement par nombre de grandes entreprises. Or, une culture du renseignement s'inscrit d'abord dans une culture (stratégique) nationale. Dans cette logique, les différences s'avèrent notables, entre des cultures asiatiques bercées par la pensée de Sun Zi ou leurs homologues anglosaxonnes fondées sur l'approche indirecte d'un Basil Liddell Hart – où l'espionnage est valorisé –, et la France où le renseignement est vu comme un mal de surcroît pas forcément nécessaire[340]. Il faut attendre la fin des années 2000 pour voir la défiance des élites politiques françaises s'estomper et le renseignement enfin être reconnu (2008) puis consacré (2013)[341].

Le fameux *cycle du renseignement*[342] a ainsi été adopté par les entreprises qui l'ont en retour enrichi pour en faire un dispositif d'information et de communication plus flexible et dynamique. « *Le renseignement, c'est l'information utile à l'action* » stipule l'amiral Lacoste. L'intelligence économique n'a, dans son volet *acquisition de l'information*, d'autres buts que de fournir aux acteurs décisionnaires des connaissances opérables à caractère stratégique. Elle forme donc bien une culture du renseignement et emprunte également à ce dernier ses méthodes. Trois modèles stratégiques procédant de différents modes opératoires traditionnels ont ainsi présidé à la fondation de l'IE, donnant lieu à un assemblage fécond : les modèles militaire, policier, et diplomatique.

| | ***Rôle traditionnel*** | ***Dynamique IE*** |
|---|---|---|
| ***Le modèle militaire*** | Attaque/défense | Cycle du renseignement (méthodologie) |
| ***Le modèle policier*** | Contrôle politique interne et sécurité physique | Sécurité économique (présence territoriale) |
| ***Le modèle diplomatique*** | Influence | Relations économiques extérieures |

**Figure 14 :** *Héritage syncrétique des modèles stratégiques de l'État qui ont influencé l'IE*[343]

[340] Voir entre autres analyses sur les cultures du renseignement : Laurent Nodinot & Marc Elhias (alias Christian Harbulot), *Il nous faut des espions ! Le Renseignement occidental en crise*, 1988, 275 p., le rapport Martre, et Yannick Pech, *L'influence du renseignement dans la formulation de la politique étrangère depuis 1991. Approche comparée de l'impact des cultures du renseignement américaine et française sur le processus décisionnel*, mémoire de M2 RISD, Lyon 3, 2013, 165 p.

[341] Fonction et priorité stratégiques du renseignement désigné comme « connaissance et anticipation », LBDSN 2008 et 2013, voir https://www.defense.gouv.fr/dgris/politique-defense/livres-blancs.

[342] Processus logique itératif fondé sur le besoin de savoir pour agir et suivant quatre étapes principales : orientation, collecte, traitement & analyse, diffusion de l'information utile à la décision.

[343] Tiré et adapté de Nicolas Moinet, *Petite histoire de l'intelligence économique. Une innovation "à la française"*, L'Harmattan, 2010, 130 p., pp. 59-65. Inspiré de Pierre Lacoste & François Thual, *Services secrets et géopolitique*, Lavauzelle, 2001, 182 p., pp. 48-71.

Le modèle militaire, le plus populaire, repose sur le besoin de connaître l'ennemi pour mieux le combattre et s'en protéger grâce au cycle du renseignement ; le modèle diplomatique, placé à la source des relations internationales, privilégie volontiers l'influence ; enfin, le modèle policier est prévu pour assurer une mission de contrôle interne et de sécurité des citoyens, pour la prévention des crimes et délits.

Ces modèles ont servi de matrice aux fonctions constitutives et intégratives de l'IE, à savoir le triptyque communément invoqué de la *veille informationnelle* (renseignement ouvert, anticipation), la *sécurité économique* (protection et prévention) et *l'influence* (proaction). Ces trois piliers peuvent se lire sur deux niveaux : le niveau géoéconomique et celui des organisations privées ; et sur deux axes : attaque/défense et gestion du risque/saisie d'opportunités.

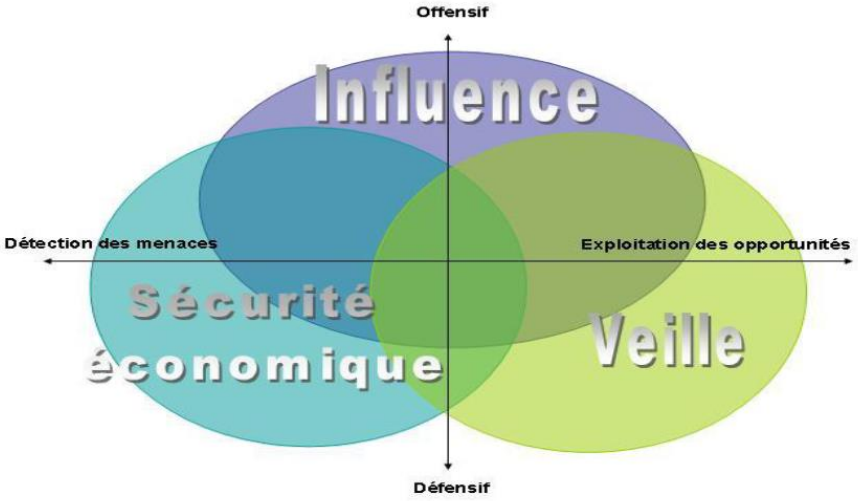



**Figure 15 :** *Les trois piliers des savoir-faire offensifs et défensifs de l'IE*[344]

La veille permet de préparer ses attaques et de détecter des menaces, mais aussi d'identifier les relais d'influence à exploiter ; c'est donc un renseignement offensif et défensif. La sécurité permet de protéger le patrimoine matériel et immatériel de l'organisation. Enfin, l'influence vise à modeler l'environnement de celle-ci à divers degrés : normatif et formel, cognitif et perceptuel. Globalement, s'il paraît plus aisé d'implémenter ce triptyque dans les entreprises sur un plan tactique, ces *modi operandi* peuvent et doivent être pensés à l'échelle stratégique de l'État, le tout dans une logique systémique. Le système (État) se compose d'unités/sous-systèmes (entreprises). La difficulté principale pour les autorités étatiques relève – outre de la masse informationnelle à traiter, protéger, exploiter et diffuser territorialement – de l'articulation des différents organes fonctionnels (armée, police, diplomatie), puisque les luttes

[344] Tiré de https://fr.slideshare.net/jdeyaref/ocdie-environnement-et-comptitivit.

d'influence bureaucratique en sus des différences de perception et d'approche génèrent souvent des batailles de chapelle[345]. Or, au sein de l'État comme au cœur d'une entreprise, l'esprit de l'intelligence économique n'admet aucune segmentation ni aucun cloisonnement.

Et précisément, il faut un liant à ce schème, dont l'enjeu réside dans l'articulation dynamique entre les trois piliers. Ce liant, c'est l'intelligence.

### e) *Une philosophie de l'intelligence*

Selon Nicolas Moinet, « *l'intelligence peut être comprise comme la capacité à jouer aux intersections*. » Aux intersections des échiquiers invisibles de la mondialisation, mais aussi à l'échelle interne d'un système organisationnel comme le montre le schéma suivant :

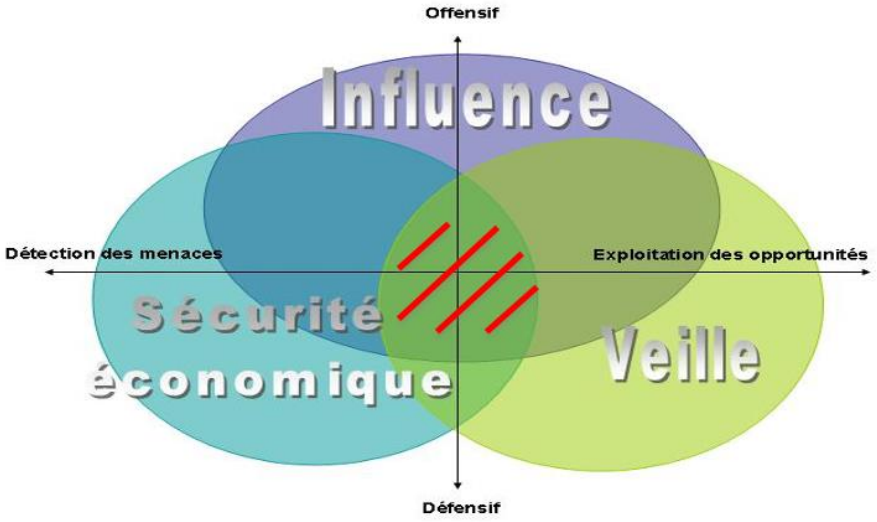



**Figure 16 :** *Orchestration des domaines de l'IE par la communication et le management de la connaissance*[346]

Légende : liant de l'intelligence collective par la communication en réseau du dispositif.

En effet, un système d'intelligence économique suppose la mise en place d'un *dispositif intelligent*[347]. Son objectif final est bien de décrypter la complexité de l'environnement de l'organisation pour l'aider à décider-agir le plus efficacement possible. L'information est au centre du concept d'IE, tel un influx nerveux ou une énergie immatérielle qui par sa diffusion réticulaire innerve le système. Et si l'on part du principe qu'il y a dissymétrie voire asymétrie

[345] Franck Bulinge, *De l'espionnage au renseignement*, *op. cit.*, *passim*.
[346] Tiré des cours de Nicolas Moinet, Université de Poitiers et de Éric Delbecque, *L'intelligence économique : une nouvelle culture pour un nouveau monde*, PUF, 2006, 224 p.
[347] Ce concept sera détaillé en section 2). Voir notamment Nicolas Moinet, « L'agilité stratégique : une question de dispositif intelligent », *Vie & sciences de l'entreprise*, 2007/1-2 (N° 174-175), pp. 142-155.

de l'information entre acteurs concurrentiels, elle constitue dès lors un avantage relatif. Certes l'information peut revêtir un caractère potentiel et dans ce sens est utile, mais elle ne constitue en réalité qu'un matériau à exploiter. Pour rendre intelligible l'environnement et agir sur lui avec acuité, il faut que l'information utile soit convertie en connaissances actionnables[348]. Ainsi, le couple information/action nécessite la création d'un sas de la connaissance dont le management forme le premier fluide des rouages de l'IE. Jeu collectif mettant en interaction les différentes fonctions de l'entreprise, l'IE harmonise et orchestre les trois domaines que sont la veille, la sécurité et l'influence dans une dynamique en réseau. L'intelligence procède par conséquent d'un dispositif réticulaire animé par la communication dont elle est la clé de voûte. De fait, le deuxième fluide des rouages de l'IE est la communication, chainon manquant entre information utile et connaissance stratégique[349]. « *Dans l'organisation*, dit Philippe Dumas, *la communication est l'acte qui met en relation les composants de l'organisme. Il n'y a pas de communication sans organisation ; pas d'organisation sans communication et pas de communication sans information.*[350] »

Au cœur du dispositif, la notion de réseau est centrale car elle désigne l'interface entre information et communication. On peut définir conceptuellement le réseau comme un processus dynamique et symbiotique multilatéral mobilisant un ensemble d'acteurs interconnectés (commutation) qui le co-façonnent par l'échange (communication-participation) d'informations dans une logique de sens (énaction[351]) et d'apprentissage (connaissances) organisationnel (projet) au service d'une finalité partagée (*ethos*/solidarité). Il y a bien sûr ici, d'un point de vue théorique, un dépassement de la cybernétique de Shannon et Wiener au profit de l'approche systémique et du paradigme constructiviste. Le réseau pouvant constituer une stratégie en soi[352], l'on appréciera d'autant mieux les réflexions posées par cet extrait du rapport Martre :

> « *L'intelligence d'un système vient de la capacité de ses éléments à se comprendre entre eux pour construire une stratégie cohérente. Plus les connexions sont nombreuses, variées, spontanées, plus le système est réactif et capable d'inventer des conduites adaptées à un environnement inattendu et complexe. Dans un monde de plus en plus turbulent, l'entreprise gagne en efficience globale et en réactivité stratégique si elle fonctionne sur le modèle du réseau : redondances pour assurer la sécurité des approvisionnements, circuits d'informations diversifiés, initiatives locales*

[348] Philippe Dumas, *Information et action*, HDR, université du Sud Toulon-Var, 1991.
[349] Nicolas Moinet, « De l'information utile à la connaissance stratégique : la dimension communicationnelle de l'intelligence économique », *Communication & Organisation*, n°35, décembre 2009, pp. 214-225.
[350] Philippe Dumas, *op. cit.*, p. 36.
[351] Fernando Varela, *«* Constructivisme et énaction *»*, École thématique CNRS, ARCo, 2006.
[352] Christian Marcon & Nicolas Moinet, *Stratégie réseaux. Essai de stratégie*, ZéroHeure, 2000, 271 p.

*encouragées, multiplication des canaux de communication avec la clientèle, ouvertures sur l'extérieur, acceptation d'autres cultures*.[353] »

Depuis 1994, le monde est encore plus turbulent et le caractère réticulaire des sociétés dans leur ensemble est de plus en prégnant sous l'influence des technologies de l'information et de la communication (TIC). Les organisations doivent donc épouser cette nouvelle donne, en premier lieu au sein des entreprises privées comme le constatent ou y invitent Christian Marcon et Nicolas Moinet.

| Organisation pyramidale | Organisation en réseau |
|---|---|
| Contrainte | Contrat |
| Obéissance | Responsabilité |
| Ordre | Désordre |
| Limitation du hasard | Risque partagé |
| Discipline | Projet |
| Information diffusée et contrôlée | Information co-élaborée |

**Figure 17 :** *Tableau comparatif des implications managériales entre une organisation hiérarchique et une organisation en réseau*[354]

Sur le plan géoéconomique, les travaux de Christian Harbulot mis en exergue par le rapport Martre nous renseignent sur les différences de posture et l'efficience des réseaux constitués par des États. La mise en regard des systèmes français et allemand en particulier est édifiante, comme en témoignent les schémas versés dans le rapport :

[353] Henri Martre, Philippe Clerc, Christian Harbulot, *op. cit.*, tiré de Dominique Genelot, *Manager dans la complexité. Réflexions à l'attention des dirigeants*, INSEP Éditions, 2011, 372 p., p. 68.
[354] Christian Marcon & Nicolas Moinet, *Stratégie réseaux...*, *op. cit.*, p. 37.

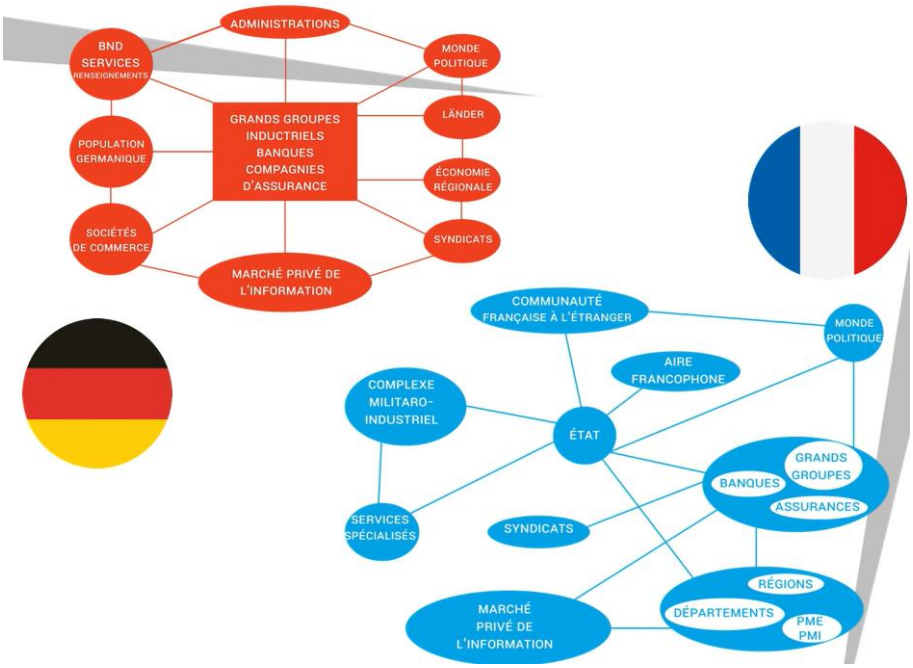



**Figure 18 :** *Schéma figurant les dispositifs géoéconomique/d'IE français et allemand*[355]

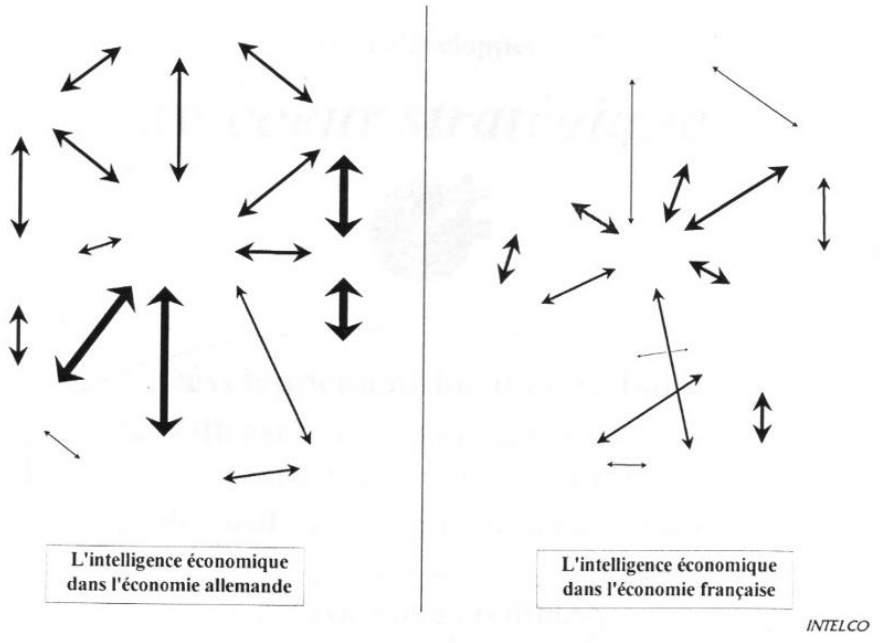



**Figure 19 :** *Maillage informationnel respectif des dispositifs géoéconomiques allemand et français*[356]

[355] « Le rapport Martre », recomposition graphique du schéma original issu du rapport Martre, vidéo diffusée par la chaine YouTube de l'IAE de Poitiers.
(https://www.youtube.com/watch?v=AhU91rSNJpM&list=PLABbIxF6MDTzSh44M3R5bxkSKl8PBvdyU)
[356] Henri Martre, Philippe Clerc, Christian Harbulot, *op. cit.*, pp. 47 et 67.

Du renseignement, production statique de l'information utile, à l'intelligence, processus dynamique de la connaissance stratégique, l'intelligence économique nous mène à la pratique de l'action d'influence.

### f) *Une pratique de l'influence*

Le savoir est le pouvoir dit la maxime. Mais le pouvoir est statique et vertical, donc le savoir inerte (informations de stock). La connaissance, à l'inverse, est dynamique ; elle est, nous l'avons dit, influence (informations de flux). Si l'« *intelligence rime avec influence* », c'est parce que la première est l'habile mise en jeu et en œuvre de la seconde pour obtenir un résultat[357]. L'influence est mouvement car c'est la production d'un influx, d'un vecteur. Influencer, c'est donc convaincre et surtout persuader son camp en interne ; et modeler, façonner l'environnement, l'adversaire en externe (influer). La démarche trouve son aboutissement dans le passage d'une vision d'un « savoir pour agir » à un « connaitre, c'est agir »[358]. En quoi consiste donc précisément l'influence ?

Deuxième étape-clé de la production législative qui va redynamiser l'IE en 2003, le rapport dit « Carayon[359] » va d'abord rappeler que l'intelligence économique souffre d'une mécompréhension conceptuelle. Tout en pointant le manque de synergie du couple public-privé et la nécessité d'infuser plus largement la notion de sécurité économique, il va appeler à une révolution culturelle fondée sur la nécessité d'élaborer une *stratégie d'influence*. C'est probablement ce troisième volet de l'outil qui forme le chainon manquant conceptuel de l'IE. Le texte propose en outre de créer un poste de Haut responsable chargé de l'IE (HRIE) en vue de diffuser la culture de l'intelligence économique. Alain Juillet, qui y sera primo-nommé en 2004, fait justement une décennie plus tard le constat d'un manque de savoir-faire en termes d'influence à tous les niveaux : étatique, territorial et entrepreneurial. Concernant les entreprises, si la situation est hétérogène mais que les grands groupes ont les moyens de tisser leurs propres réseaux d'influence, les sociétés plus petites et intermédiaires nécessitent l'appui des autorités publiques et de leur secteur économique. Quant à l'État, la théorie n'est pas suivie d'effets pratiques. À l'image des mots de l'avocat Nicolas Ravailhe prenant pour exemple les confrontations intergouvernementales franco-anglaises (lobbyisme) au sein de l'UE, « *Les Britanniques veulent gagner quand nous, Français, voulons avoir raison.*[360] »

[357] Guy Massé & Nicolas Moinet, *Petit bréviaire contre l'intelligence superficielle*, VA, 2021, 96 p.
[358] Thierry Libaert & Nicolas Moinet, « La communication, dimension oubliée de l'intelligence économique », *Communication & Organisation*, PUB, 2012/2 (n° 42), 280 p.
[359] Bernard Carayon, *Intelligence économique, compétitivité et cohésion sociale*, rapport au Premier ministre, juillet 2003 (https://www.vie-publique.fr/rapport/26501-intelligence-economique-competitivite-et-cohesion-sociale)
[360] Cité par Nicolas Moinet, *Les sentiers de la guerre économique.* T2, *op. cit.*, p. 166.

L'influence est donc une affaire de culture, et de stratégie. Si la plupart des experts de la guerre et de l'intelligence économiques s'accordent à penser que les élites politiques françaises n'ont pas encore pris toute la mesure de ces enjeux, pour cause de désarmement intellectuel et de déconnexion du réel[361], des progrès sont toutefois réalisés. Ainsi pour l'influence qui est enfin considérée comme décisive et érigée fin 2022 en sixième fonction stratégique nationale par le président Macron. En dépit d'un aspect offensif invoqué implicitement par le chef de l'État, il reste toutefois à définir ce que suppose « *promouvoir* […] *les intérêts et les valeurs de la France*[362] » ou « *Convaincre fait partie clairement des exigences stratégiques*[363] » en termes de moyens et de pratiques, quand précisément celles de l'adversaire s'exercent souvent en dehors de toute considération légale et cherchent non à convaincre (*logos*) mais à persuader (*pathos*) et fédérer (*ethos*). En tout état de cause et comme le mentionne à raison la *Revue nationale stratégique 2022*, l'influence est un outil d'expression de la puissance et un domaine de *contestation* que n'a pas manqué de mettre en exergue un an plus tôt le Chef d'état-major des Armées (CEMA), le général Thierry Burkhard. Dans sa *vision stratégique* publiée en 2021, le CEMA propose une approche renouvelée de la conflictualité en se fondant sur le credo *sunzien* de « *gagner la guerre avant de la faire*.[364] » Dans cette vision globale, le général Burkhard propose une nouvelle grille de lecture des conflits basée sur le triptyque *compétition-contestation-affrontement*. Placée à l'intersection de la *compétition* et de la *contestation*, l'influence prend ainsi toute sa dimension de levier de puissance[365]. Une question se pose néanmoins : suffit-il de répondre militairement à ces enjeux ? Certes, selon la *Revue*, la fonction stratégique de l'influence – à l'échelon international – doit être portée par le ministère de l'Europe et des Affaires étrangères. Mais l'outil ne doit-il pas être subordonné à une stratégie politique plus globale ? En d'autres termes, ne faut-il pas ériger une véritable politique de *soft power* au-delà d'une lutte de contre-influence ou d'une simple promotion de valeurs aujourd'hui largement contestées et subverties ?

[361] Voir notamment Guy Massé & Françoise Thibault, *Intelligence économique : un guide pour une économie de l'intelligence*, Bruxelles, De Boeck, 2001, 359 p. ; Christian Harbulot, « Penser la guerre économique », conférence tenue à SciencesPo Lyon, 29 novembre 2018. Le manque de courage, la chute du patriotisme et la naïveté, voire la complaisance et les compromissions sont pareillement évoqués.

[362] *Revue nationale stratégique 2022*, p. 24 (https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022, consulté le 20 juillet 2023.

[363] Extrait de l'annonce du président Macron du 9 novembre 2022 (https://www.opex360.com/2022/11/09/m-macron-erige-linfluence-au-rang-de-fonction-strategique/, consulté le 20 juillet 2023)

[364] Nous analysons cette grille de lecture dans le chapitre 4. (https://www.defense.gouv.fr/ema/chef-detat-major-armees/vision-strategique-du-chef-detat-major-armees-fresgb).

[365] Les mots employés à dessein de « stratégie de puissance nationale » (certes « d'équilibre ») par le CEMA semblent même dépasser la posture officielle mesurée des autorités publiques françaises. Aucun texte législatif ou doctrinal ne porte cette appellation hormis pour qualifier les politiques agressives de certains adversaires internationaux.

Car, comme le souligne Nicolas Moinet[366], le *soft power* est la clé de voûte de la *guerre économique systémique*. « *Ce pouvoir feutré qui enveloppe de toute part*[367] » est à la ruse et la dissimulation ce que le *hard power* est au pouvoir de la force brute. Fondé sur l'idée d'un exercice pacifique de la puissance par la voie du leadership, la séduction et l'adhésion à un modèle dominant notamment culturel, le *soft power* est en réalité plus global et insidieux. D'une part, il est plus qu'un levier d'influence culturelle, il est un instrument d'ingénierie sociale et d'emprise globale sur les esprits, avec ses tactiques d'encerclements et aveuglements cognitifs – *via* les TIC en particulier. D'autre part, le *soft power* n'est pas dissocié des autres instruments de la puissance, bien au contraire. Et si l'on associe généralement l'économie à la puissance dure, en réalité elle est duale comme le souligne Nicolas Moinet[368]. Dès lors, l'influence culturelle est indissociable de la puissance commerciale ; ne parle-t-on pas *d'industrie* et de *produits* culturels ? Or, le commerce, la culture ou l'information se diffusent de manière matérielle et immatérielle, la guerre systémique se faisant *par le contenant* (les infrastructures, les « tuyaux », la technique) et *par le contenu* (l'information, la connaissance, la technologie)[369]. De même que les États-Unis usent et abusent des *hard et soft powers*, la Chine notamment s'emploie à teinter de *soft* son *hard* voire son *sharp power* (pensons à la 5G et à TikTok, aux BATHX, instituts Confucius, *diplomaties du Panda* et du *sourire* ou des *Loups-guerriers*, *Nouvelles routes de la soie/stratégie du collier de perles*, etc.). *In fine*, le *soft power* n'en demeure pas moins une stratégie de domination, mais une domination indirecte et masquée qui s'insère *stéganographiquement* dans le paysage lénifiant de la « mondialisation heureuse », avec ses normes et principes moraux forgés par des acteurs en quête de puissance globale. On le voit, l'influence est un marqueur du niveau ou du potentiel de puissance d'un acteur sur la scène mondiale.

Au bilan, l'intelligence économique constitue bien une posture de combat et une philosophie praxéologique. Elle n'a de sens que dans l'acceptation de l'existence *a minima* d'une hyper-compétition économique, *a maxima* d'une guerre permanente et systémique. Surveillance et vigilance, sécurité et défense, proaction et influence : elle est à l'image des six fonctions de la stratégie de défense et de sécurité nationale (*connaissance & anticipation, dissuasion, protection, prévention, intervention, et influence*). Dans cette optique, ses partisans et artisans appellent de leurs vœux un traitement stratégique à la hauteur, comme le rappelle et l'augure peut-être un rapport d'information du Sénat publié en juillet 2023 et

[366] Nicolas Moinet, *Les sentiers de la guerre économique*, T2, *op. cit.*, 2020, pp. 32-40.
[367] Définition imagée du *soft power* par le stratégiste Gérard Chaliand (https://www.revueconflits.com/etats-unis-soft-power-consommation-gerard-challiand/, consulté le 20 juillet 2023.
[368] Nicolas Moinet, *ibid.*, p. 38.
[369] Christian Harbulot, *L'art de la guerre économique*, *op. cit*. ; Nicolas Moinet, *ibid.*

préconisant une posture résolument offensive dans le cadre d'une *stratégie nationale d'intelligence économique* (SNIE)[370].

Après avoir présenté les fondamentaux de l'intelligence économique, nous empruntons la définition formulée par Nicolas Moinet : « *l'intelligence économique est une dynamique collective qui vise à gagner en agilité par l'usage stratégique de l'information.*[371] » De là, il s'agit de pousser plus avant notre réflexion sur ce qui caractérise l'intelligence économique.

### 2) L'IE comme art et science de la guerre économique : caractéristiques-clés d'une stratégie-outil

« *Les seules batailles perdues sont celles que l'on ne mène pas.* »

En 2012 sortait *Le vide stratégique* de Philippe Baumard[372], présentant le monde actuel comme vidé de sa substance stratégique et assimilant les gouvernants (occidentaux) à des tacticiens de courte vue. Moins qu'une *fin de la stratégie*, c'est d'un vide qu'il s'agit pour l'auteur, un abîme continu entre les idées et leur réalité : la stratégie a glissé vers une tactique gestionnaire, fondée sur une boîte à outils de modes opératoires formatés pour traiter mécaniquement les crises. Purgée de sa riche et plurielle origine grecque et de ses *strategoi*, la stratégie est devenue clausewitzienne puis managériale, limitée, limitative. On ne pense plus donc ne construit plus l'avenir et le temps long mais on gère le présent, l'immédiat du temps réel. On n'est plus dans le stratégique mais dans l'idéologique-technologique. Philippe Baumard achève toutefois son analyse sur une pointe d'optimisme en expliquant que ce vide est amené à se remplir par une réappropriation du discours stratégique et de l'économie du réel. L'intelligence économique, en art et science de la guerre afférente n'est rien d'autre que cette intentionnalité de se réapproprier le réel, au-delà de la complaisance ou du déni ambiants. Ainsi, en tant que posture éminemment stratégique, l'IE appelle, plus que la seule description que nous avons effectuée en amont, sa caractérisation pour en tirer une grille d'analyse à même de mieux appréhender le cyber, enjeu complexe et stratégique par excellence.

[370] Marie-Noëlle Lienemann, Jean-Baptiste Lemoyne, Sophie Primas, *Anticiper, adapter, influencer : l'intelligence économique comme outil de reconquête de notre souveraineté*, Rapport d'information au Sénat, juillet 2023 (https://www.senat.fr/notice-rapport/2022/r22-872-notice.html)

[371] Voir entre autres : https://www.epge.fr/wp-content/uploads/2019/01/Nicolas-MOINET-L%E2%80%99intelligence-%C3%A9conomique-nerf-de-la-guerre-%C3%A9conomique.pdf

[372] Philippe Baumard, *Le vide stratégique*, CNRS éditions, 2012, 256 p. Il est notamment Professeur des Universités au CNAM, directeur du laboratoire Sécurité, défense, renseignement, criminologie, crises, cybermenaces (SDR3C).

L'intelligence économique n'est pas un concept monolithique. Elle est en effet traversée par quatre courants qui interprètent la réalité économique selon un prisme oscillant de l'idéalisme (diplomatie économique) au réalisme (guerre économique) en passant par le pragmatisme (sécurité économique) et l'économisme libéral (compétitivité économique).

| Guerre économique | Sécurité économique | Compétitivité économique | Diplomatie économique |
|---|---|---|---|
| International | Intranational | Public-privé | Transnational |
| Volonté de puissance géostratégique | Défense des intérêts nationaux | Néolibéralisme et mondialisation maîtrisée | RSE et développement durable |
| La guerre par d'autres moyens | La défense comme stratégie | La compétitivité comme règle | La raison comme langage |
| Conflictualité assumée | Conflictualité subie | Conflictualité non assumée | Conflictualité négociée |
| Renseignement étatique comme modèle d'IE | Le renseignement étatique comme rempart | Une IE à géométrie variable | L'IE comme écologie de l'information |

**Figure 20 :** *Tableau comparatif des courants théoriques de l'IE*[373]

Si, dans les faits, les politiques publiques d'IE en France s'inscrivent volontiers dans l'approche de sécurité économique – surtout vue comme une protection et dans un esprit traditionnel de défense –, les différents gouvernements depuis trente ans ont privilégié l'approche néoclassique de la compétitivité, suggérant que l'économie se caractérise certes par des interactions notamment commerciales de plus en plus concurrentielles et agressives, mais que ces dernières sont l'apanage d'entreprises aux stratégies mondiales et transnationales évoluant dans un marché global. Quant aux professionnels académiciens ou praticiens de l'IE, ils considèrent en revanche pour la plupart que prévaut l'interprétation polémologique et sécuritaire. C'est le choix de cette grille de lecture selon nous éclairée qui a été fait dans le cadre de nos travaux. De ce point de vue, l'intelligence économique se présente comme l'art et la science de cette guerre économique, de laquelle il faut se protéger, laquelle il faut mener. Dès

[373] Franck Bulinge & Nicolas Moinet, « L'intelligence économique : un concept, quatre courants », *Sécurité et stratégie*, 2013/1 (12), pp. 56-64. Certains éléments ont été modifiés comme les notions d'étatisme, remplacées par le qualificatif national jugé plus pertinent (État-nation).
Ces courants ne sont pas sans rappeler ceux de la théorie des relations internationales (paradigmes réaliste, libéraliste, constructiviste/critique…). L'IE française pourrait en l'occurrence s'inscrire dans l'alliage néoréalisme-constructivisme, postulant des RI régies par des rapports de puissance multidimensionnels et une réalité (co)construite plutôt que donnée, telle qu'elle est et non qu'on voudrait qu'elle soit (idéalisme libéral).

lors, ses intentions, son regard, et simplement son propos relèvent d'une posture patriote, souveraine et même inclusive, puisqu'elle est finalement la seule approche qui embrasse les trois autres dans l'esprit de la célèbre maxime « *si vis pacem parabellum* ». Se préparer au pire et construire le meilleur sans naïveté. *In fine*, l'objectif de l'IE est la sauvegarde de l'emploi par le maintien d'une compétitivité dans une économie parfois synonyme de jeu à externalités positives, mais dont le substrat se matérialise plus concrètement dans le rapport de force léonin. Somme toute, l'économie globalisée est la cristallisation de l'équilibre de Nash ou plus exactement d'un équilibre bayésien.

## Les caractéristiques-clés de l'intelligence économique

Méthodologie

Pour cet essai de modélisation des caractéristiques de l'IE, nous nous sommes appuyé sur la littérature scientifique de la discipline, l'observation des témoignages de managers et l'échange avec des professionnels de la pratique. Par ailleurs, la présentation des principes fondamentaux dans la section précédente se prolonge ou s'articule avec cette étape de modélisation. Nous avons pris le parti de décliner ces caractéristiques à deux niveaux, partant du constat que l'IE est une théorie-pratique. Le premier niveau est donc conceptuel et abstrait, le second opérationnel et concret. Il nous paraît ainsi pertinent de mettre en exergue tout autant la prégnance de la disposition (mentale) que l'importance du dispositif (opérationnel) de l'intelligence économique. Enfin, par souci d'opérationnalisation de la démarche, nous en tirerons la substance pour en dégager des caractéristiques-clés en vue de leur application au domaine cyber.

*N.B.* : bien qu'elle soit pertinente – voire plus légitime – la notion « d'intelligence stratégique » (IS) sera ici écartée pour deux raisons liées à des considérations culturelles et historiques. En premier lieu, malgré le foisonnement sémantique autour du concept d'IE et la difficulté à y trouver une définition unanime, nous nous appuyons sur l'approche d'une « école française » de la discipline qui fait autorité sur le plan académique. En effet et c'est à souligner, bien que le concept initial soit originaire des États-Unis (*organisational/competitive intelligence*), cette « patte » hexagonale a inspiré à son tour la doctrine américaine, jusqu'à y réintroduire la notion d'*economic intelligence* (EI). Dans le monde francophone voire européen (Italie et Espagne en tête), le rayonnement de l'IE a été encore plus décisif, même si on place parfois celle-ci à un échelon opérationnel tandis que l'IS aurait vocation, comme son nom l'indique, à s'insérer au niveau supérieur (cas de la Wallonie belge)[374]. En second lieu, et même si l'AFNOR a bien consacré une norme à l'IS, l'économie est tellement centrale dans le

[374] Pierre-Yves Debliquy, *Chercher n'est pas trouver*, Edipro, 2014, 323 p.

cadre d'analyse français que les autres domaines y sont subordonnés. On l'a dit, le facteur économique de la puissance est prégnant : l'économie définit la politique qui, sans la maîtriser complètement, la façonne à son tour. Aussi, économie et stratégie – donc politique – se confondent-elles. On associe souvent de fait l'*intelligence économique & stratégique*.

## *Caractéristiques théoriques de l'IE*

### *1ère caractéristique : un domaine de réflexion interdisciplinaire qui s'appuie sur le paradigme de la complexité pour appréhender le « village global »*

« *La pensée complexe n'est pas inscrite dans l'éducation.*
*On continue à enseigner une façon de penser compartimentée et réductrice.* »

Edgard Morin

Irriguée par plusieurs champs disciplinaires, l'IE est une approche par nature transversale. Science politique, droit, sciences économiques, sciences de gestion, sciences de l'information et de la communication (SIC) ont contribué à sa maturation conceptuelle et théorique. Elle est à l'image exacte de son objectif : décloisonner les savoirs, multiplier les approches et les points de vue pour en synthétiser les apports réflexifs à même de décrypter la complexité (Morin, *La Méthode*). L'IE est victime de sa propre complexité et en même temps remède pour appréhender celle du monde qui se traduit par quatre ruptures convergentes et structurantes[375] :

- une rupture méthodologique : les phénomènes concomitants de transnationalisation, régionalisation et globalisation redéfinissent les relations internationales et interpersonnelles, imposant le passage d'une économie de production à une économie de la relation-interface ;
- une rupture technologique : les TIC et la « révolution numérique » modèlent et remodèlent sans cesse nos modes de pensée et nos comportements, les territoires, l'appréhension de l'espace et du temps, jusqu'à nous influencer voire manipuler (*technologies persuasives*[376]). Dans tous les cas redéfinissent le cours de l'histoire en questionnant la singularité de l'humanité (transhumanisme, robotique, IA, NBIC…) ;

[375] Guy Massé & Françoise Thibault, *Intelligence économique : un guide pour une économie de l'intelligence*, *op. cit*.
[376] Brian J. Fogg, *Persuasive Technology…*, *op. cit.*

- une rupture quantitative : la société de l'abondance induite par le progrès technique crée toujours plus d'infomédiation et d'intermédiation et soustrait peu à peu à l'individu sa responsabilité, son autonomie voire son libre arbitre (infobésité, désinformation, *slacktivisme*…). Cette rupture engendre le passage d'une économie productive à une économie d'usages et de solutions ;
- une rupture qualitative : la dématérialisation de l'économie par l'offre de services autorise l'optimisation des coûts par l'automatisation et la numérisation (biens matériels optimisés par les modes de distribution, actifs immatériels…).

Ces quatre ruptures à la fois alimentent et résultent de l'avènement d'une société en réseaux dans le cadre de la société de l'information et de la communication, puis de la connaissance. Par-delà la vision simpliste et aseptisée d'un *village planétaire* au vrai plus proche d'une tour de Babel, l'IE opère un décryptage des « *rapports de force géoéconomiques cachés dans la lumière*[377] » en cartographiant et analysant les mouvements offensifs et défensifs des acteurs et contextualisant leurs échecs et succès économiques.

### *2e caractéristique : science en action et culture de l'intelligence rusée*

« *La mètis est au logos, en somme, ce que le savoir-faire est au savoir.* »

Robert Turcan

On l'a dit, l'IE s'inspire et relève d'une culture du renseignement. Mais elle enrichit cette trame originelle via l'ouverture paradigmatique et méthodologique qu'elle opère par rapport à un monde fermé – le renseignement d'État – au défi d'une société ouverte[378]. Comme le soulignait l'amiral Pierre Lacoste, « *Les armées et les administrations ne sont plus les premiers innovateurs, c'est le privé qui est à la pointe du progrès en matière de gestion "intelligente" de l'information utile. Les services étatiques de renseignement ont le plus grand intérêt à suivre de près ce qui se fait de mieux dans les applications civiles.*[379] » Au-delà du renseignement, processus en circuit fermé[380], l'IE vise une catégorie d'intelligence particulière dont la référence a servi de fil conducteur aux acteurs français de la discipline. Cette intelligence c'est l'*intelligence rusée*, la *mètis*. Cette notion renvoie d'une part à une figure mythologique peu connue du panthéon grec, Mètis, déesse mineure car notre héritage de la

[377] Nicolas Moinet, *Les sentiers de la guerre économique*, *T2, op. cit.*, 2020, p. 32.
[378] Franck Bulinge et Nicolas Moinet (dir.), « Le renseignement, un monde fermé dans une société ouverte », *Hermès*, 2016/3 (n° 76), 216 p.
[379] Pierre Lacoste (amiral), « Quel renseignement pour le XXIe siècle ? », in *Actes du colloque au Carré des Sciences du 3 avril 2001*, Panazol, Éditions Lavauzelle, 159 p.
[380] Il est orienté seulement vers le pouvoir politique, commanditaire non tenu d'intégrer le renseignement dans sa réflexion/ses décisions puisqu'il constitue une source d'information/de savoir parmi d'autres.

Grèce s'est focalisé sur l'approche antique platonicienne et aristotélicienne (philosophie, théorie) de l'intelligence. Or, Mètis est symbole de l'intelligence en action, elle préside aux arts & techniques, à l'invention des armes, aux feintes et aux pièges, qu'il s'agisse de chausse-trappes intellectuels (rhétorique, politique) ou pratiques (tramer, tisser, réticuler). D'autre part et justement à cet égard, *mètis* est aussi un nom commun, un caractère possible des humains. Ainsi du célèbre héros Ulysse dit *polymètis*, considéré comme l'homme de toutes les ruses, de tous les tours et stratagèmes, le combattant astucieux capable d'user de moyens au besoin déloyaux[381].

Que tirer sur un plan plus concret de ce concept ? Une disposition mentale, un état d'esprit propres à l'IE qui consistent à chercher la vérité et lire entre les lignes, à analyser l'environnement et à s'y mouler, à perturber l'adversaire par notre rhétorique (communication, mésinformation), nos stratagèmes (pièges, feintes tactiques) et notre dissimulation (*deception,* camouflage). « *Engagée dans la vie pratique,* [la mètis] *suppose un monde instable. Son terrain d'application est le devenir sensible et vivant. Elle doit se modeler sur son objet, ondoyant et multiple dans le temps comme dans l'espace, pour le dominer : d'où sa polymorphie mobile et fonctionnelle*.[382] » Nous nous situons bien dans l'intelligence–influence, la connaissance oblique des acteurs les plus adaptés et adaptables à un monde incertain et turbulent. Penser le présent, décrypter les indices, comparer, prévoir dans un état de préméditation vigilante, tel est l'esprit et le corps de la *mètis*. Les deux animaux pris en exemple pour l'illustrer ne sont pas hasardeux : le renard et le poulpe. Au premier, la commune ruse et au besoin la fourberie du prédateur ; au second, la capacité mimétique, les attributs polymorphiques et la souplesse indéniable, qui déploie ses rets pour capturer sa proie[383]. Or, c'est bien sur une logique rét-iculaire que s'appuie l'intelligence économique.

### *3e caractéristique : une posture de combat fondée sur le triptyque patriotisme–unité–souveraineté*

« *L'unité concerne autant la verticalité – être soi – que l'horizontalité – faire corps avec les autres.*
[…] *L'unité se confond avec l'existence même d'un corps collectif.*
*Il n'y a pas d'unité sans une identité commune.* »

Raphaël Chauvancy & Nicolas Moinet

[381] Marcel Détienne & Jean-Pierre Vernant, *Les ruses de l'intelligence. La* mètis *des Grecs*, Champs essais, 2018, 464 p. Voir aussi l'entretien de Jean-Paul Vernant (http://www.fabriquedesens.net/Les-ruses-de-l-intelligence-La), consulté le 4 avril 2022.
[382] Robert Turcan, « M. Détienne et J. P. Vernant. Les ruses de l'intelligence. La mètis des Grecs », *Revue de l'histoire des religions*, tome 189 - n°2, 1976, pp. 223-225.
[383] Autant de critères qui s'appliquent au couple agilité/paralysie que formalise le modèle OODA de John Boyd, sur lequel nous reviendrons.

Dans son ouvrage *Techniques offensives et guerre économique* (1998), Christian Harbulot notait déjà que la patriotisme, expression du dévouement du citoyen pour son pays, perd de son importance dès lors que l'économie devient synonyme de coopétition entre États partenaires interdépendants. Il déplore alors que cette crise du patriotisme a sapé toute velléité de puissance. Nul doute que cette perte de repères s'est aggravée depuis lors et qu'on assiste à un délitement de l'idée même de nation depuis plusieurs décennies. Si la notion n'est pas nouvelle et que Jean Arthuis dès 1997 ou Dominique de Villepin en 2005 appelait à un « patriotisme économique », les conséquences de la crise sanitaire du tournant de la décennie 2010 n'auront pas manqué de révéler les failles d'une trop grande dépendance des pays européens au marché globalisé. Discours politiques sur les relocalisation, réindustrialisation et souveraineté économique ont, en ce début de décennie 2020 et notamment en France, le vent en poupe. À cet égard, comme le note dès 2009 Pascal Lorot, « *l'initiative* [de J. Arthuis] *reste encore à ce stade pour l'essentiel purement verbale et on est fort loin des tentatives américaines de donner une portée extraterritoriale à plusieurs de leurs législations nationales destinées à restreindre le commerce avec certains États peu en cour à Washington.*[384] »

Pourtant, l'intelligence économique se comprend comme la mise en abime d'une double logique de solidarité et d'unité nationales, celle de l'État et de la nation. En effet, les intérêts ou les risques privés sont plus ou moins directement liés à l'État et peuvent ainsi servir ou léser l'intérêt général. La nation suppose la cohésion entre individus, organisations, territoires et État, ainsi que le décrit le schéma suivant :

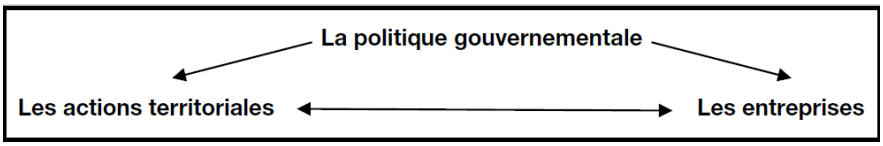



**Figure 21 :** *Les trois niveaux de l'IE*[385]

Si le nationalisme peut être entendu comme la haine des autres, le patriotisme à l'inverse est bien compris comme l'amour des siens confiait Romain Gary. Il s'agit ainsi pour l'IE d'impulser un mouvement auquel l'État emboîterait le pas par la reprise en main de sa souveraineté. Les dernières commissions sénatoriales (2021-2023) sur la souveraineté économique, énergétique et numérique du pays montrent combien cette question s'inscrit dans l'agenda politique, du moins sous l'influence des acteurs de l'IE et de rares politiques, députés ou sénateurs dans une

[384] Pascal Lorot, « De la géopolitique à la géoéconomie », *op. cit.*, §27.
[385] Alice Guilhon & Nicolas Moinet (dir.), *op. cit.*, p. 18.

logique souvent transpartisane. Bernard Carayon avançait justement que « *l'intelligence économique est un patriotisme économique* »[386], le justifiant *a minima* au nom d'une communauté d'intérêts mutuels[387] entre acteurs nationaux (État, filières économiques, entreprises et donc individus) :

> « *Je devine le sourire du lecteur à la découverte de ces mots. Que notre tropisme soit notre région, notre pays ou l'Europe, c'est pourtant ce patriotisme économique qui sera le garant de notre cohésion sociale. S'il n'en est convaincu par sa réflexion propre, qu'il examine, sans parti-pris, comment nos grands partenaires se comportent et réussissent. Le patriotisme économique n'est pas une idéologie, pas plus que l'intelligence économique n'est un concept : c'est une politique sociale.*[388] »

Le propos est significatif : le patriotisme, c'est une culture, c'est un acquis. Une culture qu'ont patiemment tissée un grand nombre des adversaires-ennemis de la France, mais aussi ses alliés-partenaires. L'unité est une sorte de synecdoque puisque si elle représente l'individu-el, elle embrasse aussi le collectif ; qu'il s'agisse d'un esprit de corps au sein d'une organisation ou d'une nation, l'objectif est le même : la recherche d'une cohérence globale et d'une intégration autour d'un projet commun ou d'une vision stratégique.

## *Caractéristiques opérationnelles de l'IE*

### *4e caractéristique : une posture managériale transversale qui place l'information au centre du jeu stratégique*

> « *L'information est devenue le moteur d'une économie dont les rouages reposent désormais sur les connaissances, les compétences, le capital social et les apprentissages de l'organisation.* »
>
> Alice Guilhon & Nicolas Moinet

Dans le marché, les acteurs économiques n'ont pas le même niveau d'information alors qu'ils sont en concurrence. Celui qui dispose de l'information – et qui sait l'exploiter et l'actionner avant ses adversaires – gagne la compétition. La guerre économique est donc une guerre – dissymétrique et asymétrique – de l'information dont l'objectif est d'obtenir un avantage concurrentiel[389]. Ainsi, l'IE part de ce constat et définit l'information comme le nœud

[386] Bernard Carayon, *Intelligence économique, compétitivité et cohésion sociale*, *op. cit.*, p. 11.
[387] Bernard Carayon, *Patriotisme économique, de la guerre à la paix économique*, Le Rocher, 2006, 243 p. Il va jusqu'à parler de fraternité : « *il n'y a pas d'intelligence économique sans solidarité d'intérêts et d'affection.* »
[388] Bernard Carayon, *Intelligence économique…*, *ibid.*, p. 11.
[389] Ali Laïdi, Conférence *Penser la guerre économique*, *op. cit.*, 2018.

de l'équation que pose la globalisation économique. Considérée avec la donnée (*big data, datasphère*) comme « l'or noir » du XXIe siècle, elle permet de nourrir la stratégie d'une institution ou d'une organisation ; mais ne peut en aucun cas se substituer à elle. Or, c'est l'authentique problème de la France selon Stéphane Mortier, qui pointe l'absence de stratégie au niveau de l'État :

> « *L'intelligence économique permet de répondre aux enjeux stratégiques à condition qu'il y ait une stratégie. Mais il n'y a pas d'attentes particulières de l'État, donc il n'y a pas de stratégie. Le SISSE a trouvé ses marques et a élaboré une stratégie, après des années de tâtonnements de la PPIE. Il est efficace dans ce qu'il fait. Mais si l'État n'a pas de stratégie à son propre niveau, c'est inutile.*[390] »

On le comprend, l'information ne prend de sens que si elle est adossée à une stratégie d'ensemble. Comprise précisément comme *le croisement de l'information et de la stratégie*[391], l'IE sous-tend nécessairement une réflexion et un positionnement clair à tous les échelons de l'État-nation ou au niveau d'une entreprise. Le schéma suivant l'illustre tout particulièrement :

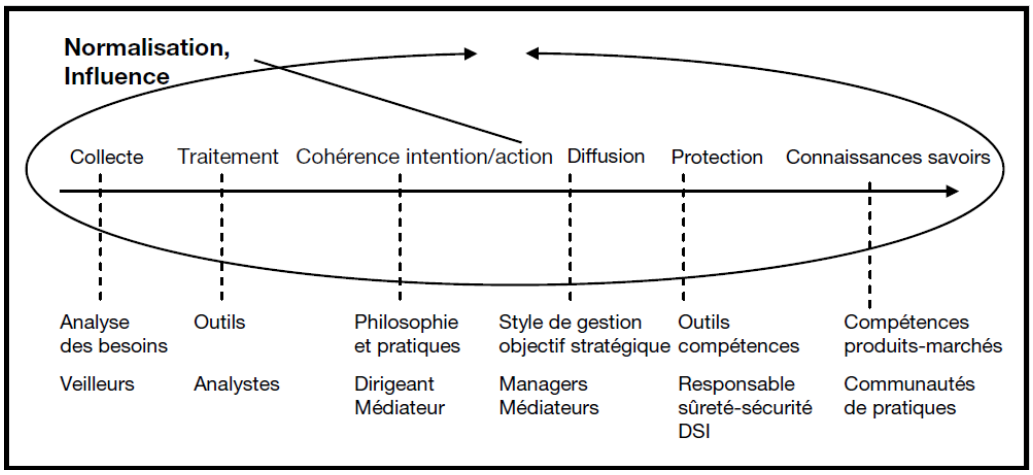



**Figure 22 :** *Le processus d'IE en entreprise*[392]

Pour que l'information soit l'influx nerveux qui traverse l'ensemble d'un système organisationnel, celle-ci doit circuler de manière harmonieuse et continue. C'est ce qui est souvent désigné par l'expression de *management de la connaissance* (*knowledge management* – KM). Selon certains professionnels, c'est cette gestion de l'information qui est

[390] Entretien avec l'auteur, 10/07/2023, spécialiste en IE, docteur en sciences de gestion, chercheur et enseignant. Il est par ailleurs membre-adjoint du Centre de sécurité économique et protection des entreprises rattaché à la DGGN. Le SISSE est le *Service d'information stratégique et de sécurité économique* issu des vicissitudes de la politique publique d'IE (PPIE). Il a remplacé la D2IE et placé la PPIE sous la tutelle du ministère des Finances de Bercy au sein de la DGE.

[391] Nicolas Moinet, *Petite histoire de l'intelligence économique…*, *op. cit*.

[392] Alice Guilhon & Nicolas Moinet, *op. cit.*, p. 16.

typique de l'IE. Plus que dans les autres fonctions avec lesquelles on l'amalgame parfois (marketing, commerce, communication), elle est, d'après Jérôme Bondu, ce qui la distingue[393]. Dans le domaine, la question est devenue une boutade : l'IE est-elle dans le KM ou le KM est-il dans l'IE ? En tout état de cause, l'IE se pose comme une synthèse d'outils et de méthodes mobilisée par une volonté au service de l'acquisition, la protection et l'exploitation de l'information. Le tout constitue le triptyque communément admis de l'IE, auquel est parfois justement ajouté un potentiel quatrième pilier, le KM. Dans les annales des citations restées célèbres, celle de l'ex-PDG de Hewlett-Packard Lewis Platt a, non sans humour, bien mis en exergue l'importance du KM : « *Si jamais HP savait tout ce qu'il sait, nous serions trois fois plus productifs*. »

Cet usage opérationnel de l'information s'est imposé à mesure que l'on comprenait l'intérêt de croiser les méthodologies civiles et militaires, comme le management stratégique d'entreprise qui dérive du commandement d'état-major. Dans les années 1960 notamment, la Harvard Business School introduit une méthode d'analyse concurrentielle basée sur le management de l'information, le modèle SWOT[394]. Dans un contexte concurrentiel de plus en plus intense, l'idée est d'inclure l'incertitude comme variable essentielle de la conjoncture économique. Suivront la matrice des cinq forces d'intensité concurrentielle de Michael Porter ou le modèle PESTEL conçu pour évaluer les facteurs politiques, économiques, sociétaux, technologiques, environnementaux et légaux pouvant impacter une entreprise. Par fertilisation croisée, ces grilles d'analyse ont inspiré les états-majors militaires avec par exemple le modèle PMESII, souvent associé aux DIME, ASCOPE ou $IRC_2$ [395].

Ainsi, l'IE se démarque par sa démarche transversale et globale et sa capacité à intégrer des méthodes et outils divers à même d'enrichir la pratique stratégique. En décentrant le regard porté sur l'économie qui s'attardait en particulier sur les critères de production et de marketing, il est plus aisé de révéler les logiques compétitives de captation et maniement de l'information. Citons le *benchmarking*, dont l'IE française a su tirer une méthode d'analyse comparée, les modèles des facteurs de concurrence des sciences de gestion (SWOT…), les méthodes d'analyse structurée (pour limiter les biais cognitifs), de mise en miroir (*red team analysis* inspirée de l'informatique) ou encore la prospective. L'IE a su aussi définir une

[393] Entretien avec l'auteur, 10/07/2023, spécialiste en IE et président de la société de conseil Inter-ligere.

[394] Le modèle SWOT pour *Strengths-Weaknesses-Opportunities-Threats* est une grille d'analyse tactico-stratégique permettant à une organisation d'évaluer ses forces et faiblesses et d'identifier les menaces ou opportunités à prévenir ou saisir surgissant de son environnement.

[395] PMESII (*Political, Military, Economic, Social, Information and Infrastructure*) ; DIME (*Diplomacy, Information, Military, Economics*) ; ASCOPE (*Areas, Structures, Capabilities, Organisation, People, and Events*) ; $ICR^2$ (*Information Collection Requirements and Information Capabilities Requirements*). Comme réserviste-spécialiste au CRR-FR (OTAN) pendant trois ans, nous avons pu notamment utiliser les grilles PMESII et DIME mais aussi le modèle SWOT. Voir notamment https://www.jstor.org/stable/27033618, consulté le 12 juillet 2023.

nouvelle méthode d'analyse, celle issue de la théorie des *échiquiers invisibles* de l'EGE. Enfin, l'IE a fait émerger par émulation des champs connexes de prise sur le réel comme ceux de l'intelligence culturelle ou juridique.

### *5e caractéristique : méthode opérationnelle globale de maitrise de l'information reposant sur trois champs d'activité : veille, sécurité et influence*

> « *L'intelligence économique peut se définir en France comme la maîtrise, la protection et l'exploitation de l'information, pour comprendre et anticiper l'environnement extérieur, ses acteurs, risques et opportunités, protéger le patrimoine informationnel stratégique et agir sur les leviers d'influence nationaux, européens et internationaux, le tout à partir de sources ouvertes et dans le respect des règles, pour in fine contribuer à créer de la valeur. Elle est souvent résumée par le triptyque veille/ anticipation, sécurité économique, influence.* »
>
> Claude Revel

Dans l'expression *intelligence économique*, il y a le mot intelligence pourrait-on arguer trivialement. L'IE, c'est donc avant tout l'intelligence des situations, une compréhension fine des marchés, des environnements, des contextes. Si cela peut paraître par trop ambitieux, elle cherche à agréger, déchiffrer et relier la multitude des informations et données issues du monde économique bien sûr, mais aussi des sphères juridique, politique, sociétale, géopolitique, technologique, voire écologique, comme autant d'échiquiers ou peut-être plus exactement de *qípán* invisibles[396]. Elle se distingue aussi par sa vocation à déceler les manœuvres souterraines que dissimulent les mouvements communs et routiniers opérés par des entités privées ou des États, voire des individus organisés en réseaux. Pour ce faire, l'IE se métamorphose en méthode fondée sur la coordination de trois activités dans un cadre légal : la veille informationnelle, la sécurité de l'information, et l'influence[397]. Cet aspect de légalité suscite encore des débats tournant autour de l'éthique des pratiques de l'IE, question à laquelle Ludovic François apporte un éclairage bienvenu[398].

*Primo*, la fonction de veille – parfois « assumée » comme *renseignement ouvert* – consiste, à l'image d'une vigie, à réduire l'incertitude de la décision en surveillant les environnements tactique et stratégique de l'organisation ou de l'État. Elle a été popularisée dans les entreprises par la célèbre règle d'or de Porter : « *Donner la bonne information à la*

[396] Le *qípán* est le nom chinois (*goban* en japonais) qui désigne le tablier quadrillé utilisé dans le jeu de Go.
[397] L'on peut opportunément se référer au document de la D2IE de 2015 sur les *Références et notions-clés* de l'IE (https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/d2ie_reference_et_notion-cle-juillet.pdf, consulté le 12 juillet 2023).
[398] Voir Ludovic François, « La question éthique dans la pratique de l'intelligence économique », *Sécurité et stratégie*, 2010/HS1 (3), pp. 43-52.

*bonne personne, au bon moment, pour prendre la bonne décision*. » Il s'agit d'un processus d'acquisition légale et d'analyse de l'information basé sur le cycle du renseignement et articulé sur l'exploitation d'un certain type d'informations. On admet généralement la typologie suivante : l'information blanche (légale, 80 à 85% de l'information globale), la grise (obtenue par des voies légales bien que parfois déloyales), et la noire (5%, obtenue illégalement et donc réservée au renseignement d'État/à l'espionnage). On en tire plusieurs axes appelés « secteurs de veille » comme les veilles concurrentielle, scientifique et technique, géopolitique, d'image/réputation, commerciale et marketing, juridique et règlementaire, etc. Placée en synergie public–privé, autorités étatiques–entreprises, la veille permet d'étudier en profondeur lesdits environnements pour anticiper les tendances, ruptures et surprises stratégiques à même de soutenir ou déstabiliser la politique étatique et le tissu socio-économique national.

*Secundo*, la fonction de sécurité économique vise à gérer les risques et ainsi protéger le patrimoine informationnel des entreprises/de l'État. Dans l'esprit des mots de l'ex-PDG d'Intel Andy Grove, « *Seuls les paranoïaques survivent*.[399] » Ainsi, la démarche consiste à auditer son entité pour identifier les risques (produit des menaces couplées aux vulnérabilités) qui pèsent sur elle afin de mettre en place des contre-mesures de sécurité et de sûreté. Eu égard à la numérisation généralisée de ce capital informationnel, il va sans dire que ces éléments sont intimement liés à la cybersécurité. Toutefois, les risques sont de natures diverses et s'inscrivent dans plusieurs champs : humain (dont les ressources afférentes, compétences interculturelles, etc.) ; matériel/physique ; immatériel comme les savoirs et savoir-faire (brevets, propriété intellectuelle…) ; normatif ; financier ; technologique ; environnemental ; réputationnel…

*Tertio*, la fonction d'influence consiste à « agir pour ne pas subir ». Elle est précisément « *la capacité à agir sur son environnement de manière à orienter les décisions des acteurs pertinents dans le sens de ses intérêts, de manière légale, sans recours à la contrainte ou à la rémunération. L'influence repose sur la conviction, l'argumentation, l'exemplarité ou la séduction. Dans la sphère économique, elle s'exerce de manière professionnelle, en amont, sur les idées, les opinions, les règles, les normes, les décisions. La capacité de mettre en place une influence stratégique est un atout dans la compétition pour les États, les territoires, les entreprises, les organisations et les acteurs de la société civile*.[400] » L'influence se décline sous plusieurs nuances : en *lobbyisme* (entreprises) sur les pouvoirs publics et en particulier les législateurs, en *plaidoyer* (ONG) auprès des opinions publiques notamment, *nudge* (influence « douce » – marketing émotionnel/sensoriel, communication publique), *diplomatie économique* ou *d'entreprise*, ou plus globalement *soft power*. L'influence est efficace car elle

[399] Andy Grove, *Seules les paranoïaques survivent*, Village mondial, 1997, 207 p.
[400] Document D2IE « Références et notions-clés de l'IE, *op. cit.*, p. 39.

est « *un pouvoir plus subtil que la force et plus avantageux que l'échange, sans récompense ni menace*.[401] »

Ces trois volets de l'IE sont conçus pour être interdépendants et leurs fonctions imbriquées. C'est au management de la connaissance qu'il revient justement de garantir leur interaction permanente et leur intégration. Par exemple, la veille sert des objectifs offensifs (l'influence) et défensifs (la sécurité). Si on ne connaît et ne comprend pas son environnement, comment espérer le façonner ? Une stratégie d'influence peut ainsi être définie comme « *une allocation de ressources informationnelles et une mobilisation d'acteurs visant à orienter les attitudes et comportements d'individus ou de publics en agissant sur leur perception*.[402] » De la même façon, si je ne protège pas ce que je sais, tous mes efforts d'influence seront réduits à néant si la réputation de mon organisation pâtit d'une fuite de données ou si la divulgation d'un procédé ou d'un savoir-faire critique ruine sa stratégie d'innovation. C'est donc par des circuits communicationnels fondés sur des réseaux socio-techniques que les organisations vont pouvoir intégrer ce triptyque pour en tirer des connaissances actionnables.

### *6e caractéristique : un processus réticulaire basé sur des dispositifs intelligents visant l'agilité stratégique*

« *Les hommes construisent trop de murs et pas assez de ponts*. »

Isaac Newton

L'IE ne pourrait mieux embrasser son environnement global qu'en lui tendant un miroir. Or, à l'image d'une *théorie des cordes*, cet environnement est désormais structuré par une trame réticulaire, le réseau. « *Pour la première fois dans l'histoire,* nous dit Manuel Castells, *l'unité première de l'organisation n'est pas un sujet, individuel ou collectif, mais le réseau. Avant cette révolution réticulaire, les faits pouvaient être rattachés à des centres : État, entreprise, groupe, individu. Désormais, ces centres sont des nœuds où se rencontrent ou s'ignorent de multiples flux d'information*.[403] »

**La caractéristique majeure de l'IE réside sans nul doute dans le principe de la mise en réseaux des acteurs d'une organisation**, à la fois passerelles interpersonnelles en interne mais aussi ponts lancés vers l'extérieur de celle-ci. Au sein d'une entreprise notamment, l'IE est « *un agrégat de compétences spécifiques au service d'une*

[401] François-Bernard Huyghe, « Les nouveaux jeux de l'influence », in *Business sous influence*, Éditions d'Organisation, 2004, 264 p., p. 208.
[402] Ludovic François et Romain Zerbib (dir.), *Influentia : la référence des stratégies d'influence*, Lavauzelle, 2015, 429 p., p. 19.
[403] Manuel Castells, *La société en réseaux – T1 : L'ère de l'information*, Fayard, 1998, 613 p.

*stratégie* » selon Christophe Deschamps[404]. Des compétences individuelles et collectives qui vont se croiser pour former des « acteurs intelligents », « agents du savoir » qui s'enrichissent mutuellement[405]. Nous l'avons dit, maîtriser l'information c'est *in fine* produire des connaissances opératives. Or, comme le disait Albert Einstein, « *La connaissance s'acquiert par l'expérience, tout le reste n'est que de l'information.* » L'expérience, fruit de l'apprentissage, vient de l'interaction d'acteurs individuels ou collectifs. Quand cette interaction est orientée vers un but et fait sens dans le cadre d'un projet commun, elle devient alors communication. Néanmoins, ces réseaux peuvent être parfois contre-productifs comme le soulignent Christophe Assens et Christelle Perrin. Notamment, si plusieurs entreprises se placent en réseaux, selon que ces derniers soient centralisés, décentralisés ou distribués, le résultat de ce partage ne sera pas le même. Ainsi, dans ces conditions, le réseau peut favoriser les échanges dans une perspective de mutualisation des connaissances ; tout comme une communication trop transparente peut à l'inverse nourrir des intérêts concurrents ou créer une relation asymétrique[406]. Rappelons plus généralement que, selon les sciences de l'information et de la communication, la communication est notamment : la mise en commun, le partage et la transmission d'informations ; l'établissement d'un lien ; un instrument-interface orienté vers un but ; et un besoin humain. Autrement dit, au-delà de n'être « *pas réductible à un ensemble d'outils ou de méthodes* » ou à « […] *une politique publique, un mode de pensée et même une culture* », l'IE est à analyser comme « *un fait social d'information et de communication.*[407] »

C'est ici qu'interviennent les notions de *dispositif intelligent* et d'*agilité stratégique*. Ainsi, on peut concevoir que l'IE est un processus dynamique et actionnable dont l'efficience peut être appréciée à l'aune du modèle de la boucle OODA[408], méthodologie analytico-décisionnelle passée du monde militaire à la sphère économique. Si l'on prend la définition dans son acception usuelle, un dispositif est, selon le CNRTL, la « *manière dont sont disposées, en vue d'un but précis, les pièces d'un appareil, les parties d'une machine* » ou un « *ensemble d'éléments agencés en vue d'un but précis* » ; et dans sa dimension militaire, un « *ensemble de mesures, de moyens, disposés en vue d'une fin stratégique.*[409] » D'une certaine façon, l'expression « dispositif intelligent » pourrait former une sorte de pléonasme. Mais croisée et imbriquée dans les SIC et l'IE, la notion prend pleinement son sens.

[404] Entretien avec l'auteur, 22/08/2017 et 17/07/2023, consultant et formateur en intelligence stratégique.
[405] Alice Guilhon & Nicolas Moinet, *op. cit.*, p. 15.
[406] Christophe Assens & Christelle Perrin, « L'intelligence économique : une stratégie de réseau pour les entreprises », *Revue internationale d'intelligence économique*, 2011/2 (Vol. 3), pp. 137-151.
[407] Thierry Libaert & Nicolas Moinet, « La communication, clé de voûte de l'intelligence économique », *op. cit.*, pp. 5-10, p. 9.
[408] Observation-Orientation-Décision-Action. Voir chapitre 4.
[409] https://www.cnrtl.fr/definition/dispositif

Dans les sciences de l'information et de la communication, le dispositif s'inscrit dans les problématiques de médiations et médiatisations (supports, modes et technologies de diffusion) et soulève le rôle de ses acteurs constitutifs et constituants (groupes, individus). On pense dès lors aux fruits de l'intelligence collective, aux interactions internes ou à la communication stratégique d'une organisation. Par ailleurs, si l'on opère un renversement du *panoptique* de Michel Foucault[410], la notion de dispositif nous amène aux TIC et à la généralisation des systèmes d'info-communication dans le cadre de la société de la connaissance et de son impératif de transparence – avec l'hyper/auto-surveillance en point de mire. L'intelligence réside là aussi dans la maîtrise de l'information et de la communication, et dans le lien social comme l'indique Daniel Peraya : « *un dispositif est un lieu social d'interaction et de coopération possédant ses intentions, son fonctionnement matériel et symbolique, enfin, ses modes d'interaction propres.*[411] » L'humain est donc au centre puisqu'il participe du/au dispositif, lequel est à la fois concret (ressources de tous ordres) et immatériel (procédures, méthodes, narratifs…) ; le dispositif se tisse dans une logique ouroborique au gré des communications entre ses membres.

Sous l'angle de l'IE, le dispositif reprend la définition basée sur les sciences de l'information et de la communication pour se considérer comme étant tout à la fois :

- une forme d'organisation et un instrument de management (stratégiquement orientés)
- un objet sociotechnique (tissu de relations sociales en interface avec des technologies d'infocommunication)
- un organe de médiations (de l'information et de la connaissance)[412].

Mais le dispositif devient proprement « intelligent » sous l'influence et par l'application des trois principes-clés de la pensée stratégique française (maréchal Foch) : *liberté d'action* (initiative et volonté) ; *économie des forces* (« être et durer ») ; *concentration des efforts* (prioriser, décider, surprendre). La notion de dispositif intelligent a été formulée par Nicolas Moinet[413] qui la fait converger avec le couple agilité/paralysie issu du modèle OODA. Ainsi, il

[410] Michel Foucault, *Surveiller et punir. La naissance de la prison*, Gallimard, 1975, 352 p.

[411] Daniel Peraya, *in* « Le dispositif. Entre usage et concept », *Hermès*, 1999/3 (n° 25), pp. 153-167. Il poursuit : « *L'économie d'un dispositif — son fonctionnement — déterminée par les intentions, s'appuie sur l'organisation structurée de moyens matériels, technologiques, symboliques et relationnels qui modélisent, à partir de leurs caractéristiques propres, les comportements et les conduites sociales (affectives et relationnelles, cognitives, communicatives des sujets.* »

[412] Typologie basée sur les enseignements en ligne de Clément Dussarps, Maître de conférences en SIC à l'université de Bordeaux (https://mica.u-bordeaux-montaigne.fr/dussarps-clement/, consulté le 3 mai 2023).

[413] Nicolas Moinet, *Dispositifs intelligents et stratégies d'innovation : la dimension stratégique de l'information et de la communication dans les réseaux de la recherche-développement*, thèse de doctorat en sciences de l'information et de la communication, université de Poitiers, 1999. Voir aussi notamment Nicolas Moinet,

s'agit de mettre en œuvre un « *système capable de scruter son environnement pertinent (veille, vigilance), de coordonner les acteurs clés (logique d'interaction) et de les inscrire dans une dynamique d'apprentissage.* » Dans ce cadre, la mise en réseau desdits acteurs[414] va permettre à une entité de prendre l'ascendant et paralyser son adversaire par la mise en œuvre concomitante des trois principes : accroître sa liberté d'action au détriment de la sienne en « l'aveuglant » ; obtenir un avantage relatif en le désorientant ; obtenir un avantage décisif pour le déborder en concentrant les attaques sur ses nœuds critiques au moment opportun.

La notion de dispositif est donc saillante dans l'IE puisqu'elle porte en elle des composantes-variables essentielles comme le réseau, la communication et l'intelligence-influence.

### *Caractéristiques-clés de l'IE*

Nous tentons ici de synthétiser les différentes caractéristiques modélisées pour en tirer graduellement la substance. En premier lieu, nous posons des mots-clés issus de notre modélisation et proposons une synthèse des caractéristiques dégagées. Ensuite, l'image d'une boussole et de ses huit points cardinaux est utilisée pour définir les orientations majeures typiques de l'IE. Enfin, sont proposées les caractéristiques-clés sur lesquelles nous fondons notre grille d'analyse des rapports entre acteurs du numérique, en transposant par la suite l'IE au champ cyber pour amorcer son opérationnalisation (section 3).

#### *Mots-clés* :

Dispositif – réseau – information – communication – connaissance – intelligence collective – influence – stratégie – gouvernance – management – praxis – processus – intégration – synergie – cohésion – méthode – outils – légal – veille/renseignement – protection/sécurité – agilité.

« L'agilité stratégique : une question de dispositif intelligent », *Vie & sciences de l'entreprise*, 2007/1-2 (n°174-175), pp. 142-155.

[414] Dans le meilleur des cas sous la forme d'un maillage infocommunicationnel et d'une synergie État-organisations/public-privé.

***Synthèse* :**

L'intelligence économique est une discipline et une pratique transversales reposant sur une culture de l'intelligence rusée collective et visant la compétitivité globale d'un État-nation-stratège. Au sein des institutions et organisations de celui-ci, elle met en œuvre, dans le cadre d'un processus communicationnel réticulaire et dynamique, un ensemble de méthodes et d'outils fondés sur la maîtrise stratégique de l'information en vue de produire des connaissances actionnables pour influencer proactivement leur environnement.

- ***La boussole de disposition mentale* :**

1- Posture et intentionnalité
2- Culture et intelligence
3- Patriotisme et souveraineté
4- Organisation et cohésion

- ***La boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité
6- Méthodes et outils
7- Intégration et synergie
8- Plasticité et agilité

***Caractéristiques-clés* :**

- L'IE se distingue d'abord par son engagement philo*sophique* et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)
- L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)
- L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

### 3) L'intelligence économique appliquée au cyber

« *Le théâtre de la guerre embrasse toutes les contrées où* [les] *puissances peuvent s'attaquer.* »

Henri de Jomini

À partir de notre appareillage théorique, nous prolongeons la réflexion vers le champ-milieu cyber. **Cette conversation entre l'IE et le cyber gage à être féconde car, placée au cœur d'une approche stratégique, l'IE permet de décentrer le regard** et d'éviter, comme en avise Bertrand Boyer, une « *vision idéaliste et centrée sur le milieu.*[415] ». En effet, on ne saurait décorréler le cyber de l'espace physique, ne serait-ce que parce que sans ce dernier, l'espace numérique ne peut exister. **Nous introduisons ici notre concept d'*Intelligence cyber* qui vient s'adosser à celui de l'intelligence économique**, et sera développé plus loin.

Le cyberespace est en première approche un milieu : il a précisément été érigé en cinquième milieu stratégique et donné lieu à un nouveau domaine de réflexion théorique et un ensemble de pratiques encore balbutiantes à travers la cyberstratégie. Comme le montre le schéma suivant, il se caractérise par sa transversalité et son artificialité : c'est le seul milieu qui ne soit pas naturel mais créé par l'Homme ; par ailleurs, il recoupe les quatre autres « territoires » avec lesquels il interagit et sur lesquels il peut donc avoir un impact.

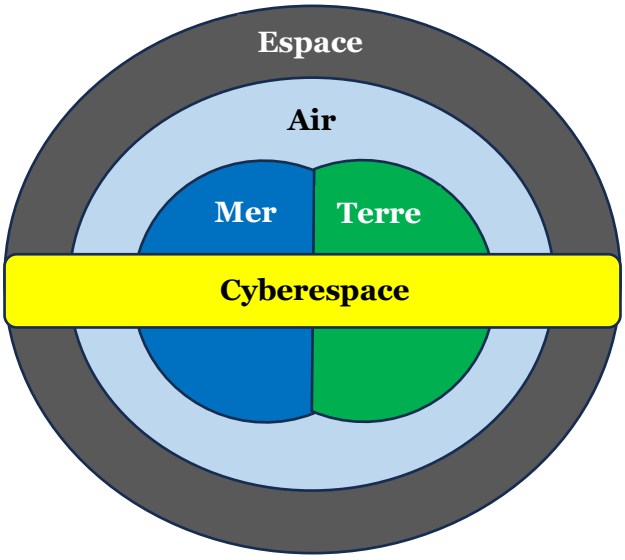



**Figure 23 :** *Les cinq milieux stratégiques*

Source : Yannick Pech, 2023.

[415] Bertrand Boyer, *Cyberstratégie. L'art de la guerre numérique*, Nuvis, 2012, 150 p., p. 29.

D'autre part, le cyber est un champ d'affrontement informationnel où les processus socio-cognitifs et les contenus sémantiques façonnent les perceptions voire les représentations des différentes sociétés humaines. Ainsi, le concept de *cyberguerre* fait l'objet d'un débat controversé et demeuré en suspens depuis qu'il a été lancé au début des années 1990. Deux chercheurs de la RAND Corporation américaine, John Arquilla et David Ronfeldt, élaborent alors une doctrine pour ce qu'ils considèrent être une nouvelle modalité de la guerre. Initialement partis de la cyberguerre – jusqu'à parler de « *blitzkrieg* du XXIe siècle » –, ils vont privilégier par la suite la notion de *guerre informationnelle* et évoquer une nouvelle forme de pouvoir, celui de la connaissance fondée sur le réseau : la *noopolitique*[416]. Le sillon de cette réflexion sur une conflictualité cyber va être plus tard emprunté par des stratégistes français.

Dans *Stratégies du cyberespace* notamment, Olivier Kempf et Stéphane Dossé fixent onze principes de cyberstratégie : sûreté ; résilience ; surprise ; contournement ; rupture ; coalescence ; chaos ; rhétorique. Déception ; fugacité de l'offensive ; asymétrie.

« Principes opérationnels permanents :

- ***Sûreté* :** ensemble cohérent de mesures mises sur pied et appliquées dans le but de maintenir la sécurité.
- ***Résilience* :** capacité du réseau à continuer de fonctionner malgré des pannes ou des attaques.
- ***Surprise* :** action prenant l'adversaire à l'improviste.
- ***Contournement* :** évitement des points forts et focalisation sur les points faibles.
- ***Rupture* :** exploitation des failles en vue de la dislocation.
- ***Coalescence* :** réunion d'acteurs disséminés et de nature parfois différente en vue d'une action conjuguée.
- ***Chaos* :** stabilité et prédictibilité du comportement des parties des réseaux durant un cadre espace-temps limité ; instabilité et imprédictibilité à moyen et long termes.
- ***Rhétorique* :** discours accompagnant l'action conflictuelle.

Principes complémentaires :

- ***Déception* :** comportement visant à cacher, plus ou moins, son action.
- ***Fugacité de l'offensive* :** une attaque soit l'emporte rapidement soit cesse.
- ***Asymétrie* :** pouvoir égalisateur du cyber, permettant à des acteurs de forces conventionnelles dissymétriques ou non-conventionnelles de lutter dans le milieu cyber.[417] »

[416] John Arquilla & David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, RAND corporation, 1999, 102 p. Parfois appelée « géopolitique de la connaissance », la noopolitique s'inspire du vocable iréniste inventé par Pierre Teilhard de Chardin quand il imagine un monde de cerveaux interconnectés dans une sphère de la pensée humaine, la *noosphère*, complément de la biosphère. Les auteurs estiment que le pouvoir coercitif est improductif et qu'en s'appuyant sur des leviers tel le *soft power*, il est possible d'imprimer une influence normative et morale par l'attraction et la séduction.

[417] Stéphane Dossé & Olivier Kempf (dir.), « Les principes stratégiques du milieu cyber », *Stratégies dans le cyberespace*, *op. cit*., pp. 181-188.

Bien que de l'aveu même des auteurs, ces principes correspondent plus à des propositions, il est à noter qu'ils peuvent recouper partiellement ceux de la doctrine classique de la stratégie (Foch), même si certains sont appréciés à l'aune de leur dimension strictement technique (réseaux *informatiques*). Ils rentrent de fait dans la sphère de l'intelligence économique, et nous pouvons à ce titre montrer leur concordance :

- ***Sûreté* :** facteur de sécurité ; se fond dans le domaine de la sécurité économique.
- ***Résilience* :** pris au sens humain et organisationnel, trouve facilement son pendant politique (État) et économique (entreprises).
- ***Contournement, rupture & surprise* :** économie des forces et souplesse, avantage relatif ; concentration des efforts sur les points faibles, avantage décisif.
- ***Coalescence* :** maillage d'acteurs (réseaux) aux intersections des échiquiers invisibles (ex. : pour une entreprise, exploiter des acteurs de l'échiquier social pour mobiliser une opinion publique).
- ***Chaos* :** gestion du désordre, de l'incertitude et des turbulences de l'environnement global.
- ***Rhétorique* :** communication, narratifs, discours masquant le conflit et les attaques.
- ***Déception* :** dissimulation et camouflage de ses actions offensives et de ses intentions.
- ***Fugacité de l'offensive* :** dans le cadre de la boucle OODA, on peut considérer que la fugacité des manœuvres est une option, mais qu'elle s'insère volontiers dans une série d'offensives diversifiées et récursives sur des temps variables (potentiels de situations).
- ***Asymétrie* :** asymétrie lors du jeu transversal sur plusieurs échiquiers invisibles (déplacer l'affrontement sur un autre échiquier/champ que celui auquel s'attend et s'insère l'adversaire).

On le voit, ces principes se prêtent bien à leur transposition bilatérale. Revenons dès lors à notre modèle des caractéristiques de l'IE pour en tester la pertinence. Le cyberespace peut être considéré comme le prolongement du monde physique et leur articulation se fait d'ailleurs sur des infrastructures matérielles. Dans ce sens, il est admis que ce milieu comporte des caractères similaires voire conjoints avec la réalité non électronique. Voici les caractéristiques établies par Bertrand Boyer de sa principale composante, l'Internet :

- Vocation essentiellement marchande (économies numérique et de l'attention, capitalisme de surveillance) ;

- Contrôle ou influence monopolistique américaine – à tendance oligopolistique – des infrastructures (câbles transatlantiques/transpacifiques, serveurs racines DNS…) pratiques, normalisation et gouvernance de l'Internet ;
- Fragmentation oligopolistique de ressort mercantile de l'Internet/du web remettant en question la *neutralité du réseau*/du Web (disposition fédérale de la FCC américaine de 2017, GAMAM, RSN, moteur de recherche Google, pages web et langue véhiculaire anglosaxonnes, BATHX chinois…) ;
- Problématique de la résilience technique du réseau (explosion du nombre d'utilisateurs humains et automates, des contenus sémantiques, capacités de stockage et de transmission de données) ;
- Sécurité des réseaux (et par extension des terminaux, des contenus), problématiques de la disponibilité, confidentialité, intégrité des données et informations. Cette sécurisation n'a pas été réalisée ni pensée par défaut lors de la création de l'Internet ou d'autres réseaux de télécommunications (incompatible avec son esprit de partage initial). Pouvoir égalisateur du cyber également en termes de sécurité[418].

La dimension marchande et ses tendances monopolistiques nous ramènent évidemment à la notion de guerre économique. La recherche de suprématie des États-Unis sur le numérique fait écho à celle qu'ils tentent d'exercer et maintenir sur l'économie mondiale. Enfin, la sécurité du numérique est à inscrire dans les mesures de sûreté que l'on cherche à établir dans le cadre de la sécurité économique.

Reprenons les caractéristiques de l'intelligence économique :

- *Disposition mentale*

**1ère caractéristique : un domaine de réflexion interdisciplinaire qui s'appuie sur le paradigme de la complexité pour appréhender le « village global »**

Ce que nous définirons plus tard comme étant une *intelligence cyber* peut opportunément s'inscrire dans le domaine de réflexion interdisciplinaire qu'est l'IE. Comment mieux appréhender le « village global », expression de l'interconnexion et de « *l'interdépendance nouvelle qu'impose l'électronique* » chère à Herbert Marshall McLuhan[419], si ce n'est en décryptant les mystères du cyberespace, ensemble systémique complexe s'il en est. Bien que le

[418] Bertrand Boyer, *Cyberstratégie…*, *op. cit.*, pp. 42-44. Nous avons amendé/adapté les propos.

[419] Sociologue canadien qui à travers sa formule de « village global » avait imaginé – avant même la création de l'Arpanet/Internet en 1969 – ce que l'on appelle aujourd'hui la société de l'information. Voir Herbert Marshall McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man*, University of Toronto Press, 1962, 294 p.

préfixe *cyber* soit issu de la vision théorique et linéaire de l'information de Norbert Wiener[420], l'espace numérique est devenu plus qu'une « machine » dont on pouvait auparavant à peu près « gouverner » et comprendre les règles de fonctionnement. Désormais, au-delà de l'électronique, du numérique et de ses éléments tangibles déjà compliqués, le cyberespace est devenu un champ informationnel et socio-cognitif où l'humain se lie à l'immatériel.

#### 2e caractéristique : science en action et culture de l'intelligence rusée

Olivier Kempf a dit que le cyberspace était un milieu de stratégie indirecte par excellence, où l'intelligence pouvait le mieux se manifester[421]. Cet espace totalement créé par l'Homme est très récent : on le construit en même temps qu'on le pense. Raison pour laquelle il nous échappe largement, générant la perception d'un désordre, au moins si l'on sort des sentiers battus du *web surfacique*. Les hackers en sont d'ailleurs la meilleure expression puisqu'ils contournent sans arrêt les mécanismes du cyberespace pour en maîtriser un tant soit peu le fonctionnement et en détourner ainsi les usages. Les cyberattaques, difficiles à attribuer, démontrent par ailleurs à quel point la ruse est de mise lorsqu'on évolue dans ce milieu. Sans parler des très concrètes offensives informationnelles visant à orienter, manipuler, façonner les opinions publiques à travers la mé-/désinformation. Sans cela même, par défaut, la technologie ou la donnée (contenu) n'est jamais neutre ; elle co-détermine la façon dont un média (social) ou une intelligence artificielle va se développer. *Mètis* est considérée comme la déesse des médecins et des marins. Tout un symbole quand on pense aux « diagnostics » réseau ou système, et à la « navigation » web : l'internautique.

#### 3e caractéristique : une posture de combat fondée sur le triptyque patriotisme–unité–souveraineté

Les technologies avancent toujours plus vite que la gouvernance juridique ou politique. De fait, les États ont un temps été écartés des avancées du cyber et notamment de l'Internet. Néanmoins, depuis deux décennies ils reprennent leurs droits et une forme de contrôle sur cet espace à première vue déterritorialisé. Pourtant, au-delà des aspects logiciels des noms de domaines de premier niveau basés sur les pays, qui ne traduisent aucun droit souverain[422], l'Internet est bien fragmenté d'un point de vue physique/territorial (câbles, réseaux informatiques, routeurs…), et donc politique. Le cyberespace peut être vu comme un milieu

[420] La théorie de l'information de Claude E. Shannon a été pensée par un mathématicien dans le cadre de la communication entre machines et du traitement du signal. Même si Norbert Wiener embrasse les êtres vivants dans la cybernétique, lui et Shannon ont donc une approche technique de l'information. De ce point de vue informatique, la théorie de l'information est donc encore valable.

[421] Olivier Kempf, *Introduction à la cyberstratégie*, *op. cit.*

[422] Les ccTLD (*country code Top-Level Domains*) symbolisent plus qu'ils ne matérialisent l'appropriation du Web par les États. Le nommage des sites web ne correspond pas automatiquement à la localisation géographique des serveurs les hébergeant. On peut le constater avec les sites des ministères français (.fr) par exemple, dont les données sont hébergées sur des serveurs en territoire américain.

mi-lisse mi-strié car il repose pour ses couches basses (infrastructures) sur des espaces maritimes et terrestres, et pour sa couche haute sur une réalité transcendante – donc a-territoriale). S'il n'existe pas de « gouvernement » ni de droit codifié propre à l'Internet notamment, certains pays, États-Unis en tête, y exercent une influence culturelle, technique, sociale, économique et normative majeure (maîtrise des contenants – câbles, et en très large partie des contenus – Web). Les « géants du numérique » ont acquis une telle influence que celle-ci se convertit parfois en quasi-puissance politique. Mais ils restent subordonnés à des législations même imparfaites. Par exemple, quand les États européens essaient d'imposer les GAMAM ou appliquent à d'autres blocs régionaux des réglementations telles que le RGPD* ou le *Digital Services Act* (DSA), il est bien question d'enjeux de souveraineté (sur les contenus). De même, quand des opérateurs chinois de câbles sous-marins de télécommunications (acheminant la fibre optique) essaient de contourner les manœuvres d'évincement par les États-Unis sur les marchés de maintenance ou de dépose (contrôle sur les contenants)[423].

- *Dispositif opérationnel*

#### 4e caractéristique : une posture managériale transversale qui place l'information au centre du jeu stratégique

L'information, dans ses acceptions techniques (notamment informatique et données) et immatérielle (contenus sémantiques), forme l'enjeu de l'espace numérique. La gestion de ces formes d'informations est une préoccupation de l'IE, dont les champs d'application connexes tels que la *Business Intelligence* (BI[424]) tentent de s'emparer. Il nous semble toutefois que l'IE est plus centrée sur l'apport de l'humain – bien qu'augmenté par des outils – et qu'il s'agit surtout de sélectionner avec soin et manager finement toutes les sources d'informations ou de données disponibles (*smart data*). La numérisation des organisations a (ré)imposé le concept de système d'information (SI), lequel comporte un volet humain (organisationnel et social) et un volet technique (informatique, stockage et réseaux de télécommunication). Cette révolution organisationnelle est à mettre en regard des trois couches du cyberespace, où l'on retrouve les différents niveaux d'une entité : la couche technique des liaisons et réseaux matériels, la couche logique de transition vers la couche humaine de réseaux sociaux, au sens premier du terme.

[423] Pour plus de précisions sur la géopolitique et la géoéconomie des câbles sous-marins, voir Camille Morel, *op. cit.*, pp. 73-149.
[424] Informatique décisionnelle basée sur l'exploitation analytique de grandes bases de données.

### 5e caractéristique : méthode opérationnelle globale de maitrise de l'information reposant sur trois champs d'activité : veille, sécurité et influence

Il va sans dire que la révolution numérique et l'accessibilité toujours plus développée aux TIC (Web, IoT) a révolutionné les métiers de la documentation et de l'information dont l'IE tire ses origines. Celle-ci est, de fait, loin d'être dépaysée, puisqu'elle a baigné dans la numérité et en a tiré tout le parti. Elle accompagne ou engendre donc naturellement de nouveaux outils d'acquisition ou de métiers comme celui de veilleur ou d'analyste, exposé à des sources infinies d'informations. Ainsi, l'IE prolonge dans le cyber sa vocation au renseignement d'une part : le renseignement d'origine sources ouvertes (OSINT en anglais) se greffe à la veille pour former une vigie bicéphale ; la cybersécurité/SSI[425] devient le pilier principal de la sécurité économique (capital informationnel) ; enfin, l'influence passe inévitablement et dans une écrasante proportion par des vecteurs numériques, notamment via les RSN dont le socle infrastructurel des réseaux informatiques est obligatoire. Le tout est canalisé par les systèmes d'information et catalysé par les TIC.

### 6e caractéristique : un processus réticulaire basé sur des dispositifs intelligents visant l'agilité stratégique

Ici aussi, les réseaux humains se prolongent dans les réseaux informatiques et socionumériques. Comme le soulignent John Arquilla et David Ronfeldt, « *la technologie renforce le réseau comme structure sociale. La révolution de l'information favorise les formes d'organisation en réseau en même temps qu'elle mène la vie dure aux structures hiérarchiques*.[426] » Un dispositif intelligent reposera donc de plus en plus sur la gestion d'un système d'information, ensemble sociotechnique cohérent et cohésif capable d'agilité. Le cyber devient ainsi le meilleur ennemi de l'organisation car cela implique une discipline pour prévenir biais cognitifs, vision technologiste et tyrannie de l'instantanéité. Mais il peut également favoriser l'horizontalisation managériale, la déconstruction des réflexes conditionnés de contrôle, et le décloisonnement des silos organisationnels. En maîtriser les rouages techniques et info-communicationnels constitue donc un avantage concurrentiel en soi pour mener la guerre systémique.

[425] SSI : sécurité des systèmes d'information, partie subséquente et plus spécifiquement opérationnelle de la cybersécurité avec laquelle on l'amalgame souvent.

[426] Interview de David Ronfeldt et John Arquilla (https://www.lemonde.fr/archives/article/1999/06/09/les-doux-penseurs-de-la-cyberguerre_3554633_1819218.html, consulté le 10 août 2023).

### *Caractéristiques-clés*

- *L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)*

On l'a vu, une stratégie globale est nécessaire à tout État-nation. Aussi, ce qui vaut sur le plan économique vaut aussi sur le plan du numérique. Il en va donc de l'autonomie stratégique de l'État de concevoir certes une stratégie cyber, mais plus largement – comme nous le discuterons – « d'implémenter » une *intelligence cyber*. Ce faisant, la question de la *souveraineté numérique* est posée à l'image de son pendant économique. Prenons l'exemple du *plan Calcul* initié en son temps (1966) par le général de Gaulle et inopportunément avorté. La France avait les atouts pour garantir, à l'image de l'énergie nucléaire, une autonomie européenne et des performances dans le secteur de l'informatique, des TIC et plus globalement de l'économie numérique. L'intelligence de la situation revient aujourd'hui à décrypter et comprendre les mécanismes d'influence passant par les TIC, lesquelles sont largement alimentées par les États-Unis, notre pire ami[427].

- *L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)*

Y compris sur le plan légal et avec les limites que cela comporte, un État démocratique et ses entités économiques doivent pouvoir lutter à armes égales dans la guerre pour, par et contre l'information que génère la conflictualité économique et qui se manifeste désormais dans son prolongement cyber. L'IE s'applique donc ici encore, dans son apport de synthétisation stratégique en termes de panoptique, cybersécurité et cyber-influence. Prenons l'exemple d'entreprises souscrivant les solutions ou services de consultants en sécurité numérique mais négligeant d'une part, les aspects non informatiques de la sécurité, d'autre part la dimension éminemment humaine de celle-ci. La sécurité ou plutôt l'insécurité de l'information apporte son lot d'illusions à des entités focalisées sur le seul volet technique de la question.

- *L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).*

Un État-stratège doit chercher à mettre en synergie tant ses propres organes que les sous-systèmes que forment les entreprises de son tissu économique. Une meilleure compréhension des mécanismes informationnels à l'œuvre dans le cyber est nécessaire, notamment en ce qui concerne les opérations d'influence, car il est devenu le support-vecteur privilégié des communications humaines. À l'instar des commandements de la stratégie de milieu :

[427] Christian Harbulot, Lucie Laurent, Nicolas Moinet, *Guerre économique : qui est l'ennemi ?*, Nouveau monde, 2022, 228 p.

contrôler, acquérir, conserver, exploiter – relativement – le cyber[428]. Le fondement de ce méta-territoire, c'est le réseau dont l'Internet est le noyau et le bien-nommé « réseau des réseaux ». Entre *effet de levier réticulaire* et *point de bascule* des mouvements d'opinions et de perceptions ainsi que *stratégies-réseaux* des « déclencheurs[429] », la vocation interdisciplinaire de l'IE est de mise pour en décrypter les logiques. Par ailleurs, la sollicitation de hackers éthiques sur un mode projet pourrait se révéler bénéfique, tant au niveau de l'État qu'à celui des entreprises qui, elles aussi, nécessitent de décloisonner leurs propres organes fonctionnels. En particulier, l'ouverture des différents départements des organisations au service informatique fait souvent défaut, comme nous le verrons plus loin. Les métiers communiquent peu ou pas (incommunication) voire plus (acommunication)[430].

Le cyber est donc « *un morceau de monde supplémentaire*[431] » où la stratégie non seulement s'applique mais joue à plein. Un monde où l'IE peut tenir un rôle fécond par sa disposition mentale et son dispositif opérationnel. La cyberguerre – au sens large – devient une sous-partie de la guerre systémique. La cybersécurité s'inscrit indiscutablement dans l'IE, ce d'autant plus qu'au moment où cette dernière naît en France, le cyber devient irrémédiablement un théâtre d'ombres et d'opérations marchandes, militaires/militarisées et psychocognitives. « *It's the economy stupid* » : les mots de Bill Clinton résonnent toujours autant en ce début de décennie 2020. D'aucuns pensent que le péché originel de l'Internet est le point de bascule entre un projet éminemment scientifique et technique de 1969 à 1994, et son dévoiement à partir du 12 avril de cette même année. Le 12 avril 1994, en effet, deux avocats américains ouvrent la boîte de Pandore en diffusant le premier *spam* de l'histoire du Réseau : une publicité pour la loterie. La réponse, en forme d'offensive cyber, ne se fit pas attendre : ce fut la première attaque – involontaire – par déni de service[432].

[428] Bertrand Boyer, *Cyberstratégie…*, *op. cit.*, p. 30.

[429] Analogie entre épidémie sociale et épidémie virale de Malcom Gladwell, *Le Point de bascule. Comment faire une grande différence avec de très petites choses*, Flammarion, 2016, 220 p. Les « déclencheurs » sont des leaders d'opinion dotés de qualités socio-relationnelles certaines et disposant de réseaux sociaux « humains » étendus.

[430] Dominique Wolton, « Communication, incommunication et acommunication », in *Les incommunications*, *Hermès*, 2019/2 (n° 84), pp. 200-205.

[431] Expression de Stuart Russell, professeur d'informatique à l'UC Berkeley.

[432] Shimon Dotan & Charles Ferguson, *Cybermonde. Le monde d'aujourd'hui*, film documentaire, Arte, États-Unis, 2023, 1h39. Anecdote citée par Leonard Kleinrock, professeur d'ingénierie informatique à l'UCLA, pionnier de l'Internet et co-créateur du datagramme avec Louis Pouzin.

# Chapitre 4 | Le constat d'une guerre cyber

« *La cyberguerre n'aura pas lieu, mais il faut s'y préparer.* »

Michel Baud

Le cyber, ça sert, *aussi*, à faire la guerre. C'est du moins la réponse qui pourrait enfin trancher le nœud gordien du polémique débat sur la « cyberguerre ». Lancée à partir de la publication d'un article de Thomas Rid qui niait la potentialité d'un tel type de conflit[433], la controverse porte encore de nos jours sur l'hypothèse d'une guerre autonome dans le milieu cyber d'une part, et sur la nature de la réponse, militaire ou non, à lui apporter d'autre part. Du fait même de la dimension artificielle du cyberespace, le problème soulevé est en effet épineux. Peut-on considérer qu'à une cyberattaque au moins critique peut être appliquée une riposte militaire conventionnelle ? Ces questionnements ne sont pas restés circonscrits à un huis clos académique d'experts de la chose militaire ; des États s'en sont emparés à travers une réflexion sur la cyberstratégie.

Le principal contradicteur de Thomas Rid est Peter W. Singer[434], qui admet plus volontiers la possibilité d'une cyberguerre, considérant que celle-ci requiert l'usage conjoint d'armes numériques et de leurs homologues conventionnelles. Par ailleurs, au regard du droit la cyberguerre n'existe tout simplement pas, car il n'y a pas de consensus ni de traité internationaux pour la qualifier. Enfin, le Centre d'excellence en cyberdéfense de Tallinn estime à ce jour qu'une cyberguerre doit combiner trois paramètres : elle se déroule conjointement à une attaque physique ; elle peut être imputée à un gouvernement spécifique ; elle cause des dégâts – sans autre précision[435]. Premier point : c'est le cas pour tous les conflits impliquant des pays développés ; deuxième point : l'attribution de cyberattaques est précisément le point le plus difficile à établir en termes juridiques ; troisième point : de quels types de dégâts s'agit-il ? Comme nous l'avons déjà mentionné, des attaques cyber-physiques ont déjà eu lieu. Par ailleurs, les attaques contre des SI, tels ceux des hôpitaux ciblés par des rançongiciels, peuvent entrainer des répercussions indirectes particulièrement dangereuses. En fin de compte, la cyberguerre n'aura peut-être pas lieu, mais la guerre ne se fera plus sans un volet cyber.

Dès lors que le cyberespace est considéré, cette fois unanimement, comme un milieu de la stratégie, il réclame une stratégie particulière. Partant du principe très généralement admis

[433] Thomas Rid, « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n°1, octobre 2011.
[434] Allan Friedman & Peter W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know®*, Oxford University Press, 2014, 320 p.
[435] CCDCOE, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, 638 p.

qu'une guerre exclusive au milieu cyber est improbable, l'espace numérique demeure toutefois un champ transversal aux autres milieux qu'il recoupe et prolonge. Sans remettre en question les principes et buts classiques de la guerre, il n'en révolutionne pas moins les usages, notamment parce qu'il fait converger progressivement les différents champs et domaines de la conflictualité. Autrement dit, « *il ne s'agit pas d'une autre guerre mais de la guerre conduite avec d'autres moyens*.[436] » Or, en s'inscrivant dans le constat d'une guerre systémique, on peut postuler que les confrontations ne sont plus seulement militaires, elles sont aussi voire surtout civiles dans certaines parties du globe. Si la « *conflictualité numérique*[437] » ne révolutionne pas les trois activités de la guerre traditionnelle : espionner, subvertir, saboter, elle les projette dans la sphère civile et peut même à l'occasion prendre des formes cinétiques. L'enjeu final se situe probablement dans l'impact et les modalités de cette conflictualité : l'espace numérique en autorise à tout le moins une application tactico-stratégique qu'on pourrait qualifier de *cyberguérilla*.

[436] Bertrand Boyer, *Cyberstratégie*, *op. cit.*, p. 79. Bertrand Boyer ne considère toutefois, à tort nous semble-t-il, que l'aspect militaire du sujet.

[437] Expression proposée par Stéphane Taillat ou Julien Nocetti, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018/2, pp. 15-27, pour qui le contournement euphémistique du terme « guerre » permet d'associer les sphères civile et privée à cette conflictualité.

## A. *Une guerre cognitive, informationnelle et informatique*

« *Gagner la guerre avant la guerre.* »

Général Thierry Burkhard

S'il n'y aura vraisemblablement pas de « cyber-Pearl Harbor » du moins en termes de destruction, l'effet de surprise tactique associé, lui, pourrait bien et a déjà peut-être été constaté à la faveur de certaines attaques numériques. Sans nier tout l'intérêt que revêtent les interprétations théoriques et tentatives de modélisation de la guerre informationnelle ou de la cyberguerre sous un angle militaire[438], il nous semble opportun de nous centrer sur une approche plus globale et axée sur la notion de guerre (économique) systémique. En tout état de cause, nous faisons le choix de l'expression « guerre de l'information ». En premier lieu, parce qu'elle fait relativement consensus entre les tenants de l'IE en France et des spécialistes de la guerre militaire[439]. En deuxième lieu, parce qu'elle s'insère dans l'intelligence économique. En dernier lieu, parce son concept apparaît en creux comme décisif dans la vision, inédite en France, du général Burkhard qui préconise de *gagner la guerre avant de la faire*.

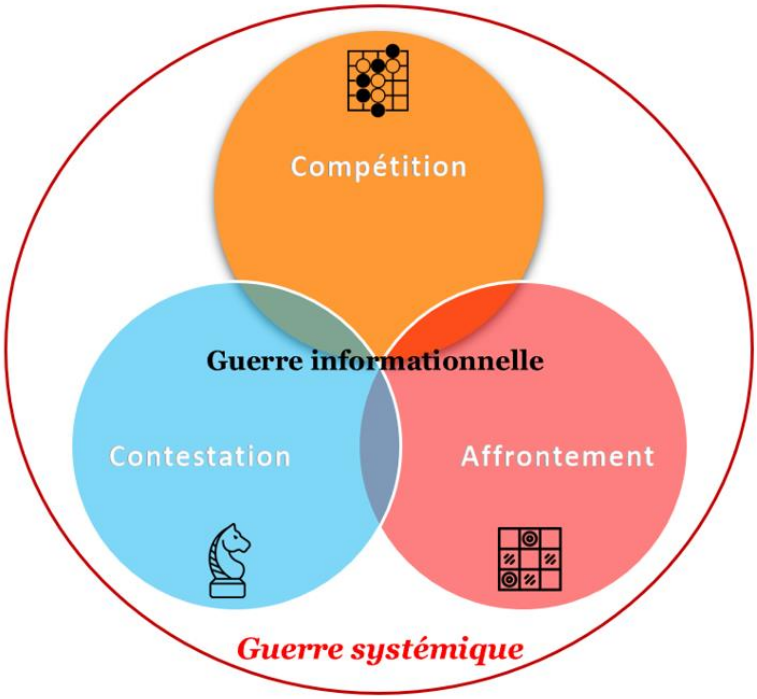



**Figure 24 :** *Le triptyque Affrontement–Contestation–Compétition de la guerre systémique*[440]

[438] L'on compte un nombre important d'expressions autour de la notion de conflit lié au cyber : guerre réseau-centrée, info-centrée, *netwar*, cyberguerre (*cyberwar/cyberwarfare*), guerre informatique, guerre de l'information…

[439] Citons François-Bernard Hughues, Bertrand Boyer, Nicolas Arpagian (à quelques nuances près) entre autres.

[440] Schéma-synthèse personnel inspiré de la Vision stratégique du CEMA, « Audition du Général d'armée Thierry Burkhard par la commission de la défense nationale et des forces armées le mercredi 23 juin 2021 », *Assemblée*

Le schéma *supra* se base sur la vision du CEMA et y associe l'interprétation imagée de jeux d'échiquiers proposée par Raphaël Chauvancy. Dans sa vision consistant pourtant à préparer la France à la guerre de haute intensité, le CEMA Burkhard envisage la conflictualité comme un ensemble de rapports de force plus strictement militaires et, ce faisant, brise un tabou français, celui de l'affrontement sous le seuil du feu, en d'autres termes une *guerre non léthale*. C'est, d'une certaine manière, l'adoubement du paradigme d'une guerre systémique. En premier lieu, sa vision sonne le glas de l'approche séquentielle traditionnelle *paix–crise–guerre* pour la remplacer par le continuum *compétition–contestation–affrontement*. Si ce dernier élément est tout à fait conforme à l'approche militaire de la belligérance, les deux premiers en revanche se marient fort bien à la conflictualité économique et informationnelle.

- *L'affrontement* renvoie au choc frontal de la guerre dans sa définition la plus stricte qui met aux prises des forces armées. Il correspond à la traditionnelle dialectique ami|ennemi et est ici symbolisé par l'échiquier du *jeu de dames*, « *dont le but de deux ennemis identifiés est d'éliminer les pièces adverses*.[441] » C'est l'*ultima ratio* du litige interétatique et le règne de la *destruction*.

- Le deuxième volet est la *contestation*, le conflit couvert et indirect fait de combats par *proxies* (procuration), de mesures coercitives (diplomatiques, économiques), d'attaques informatiques sur le contenant et informationnelles sur le contenu (narratifs, campagnes de mé-/désinformation, subversion). C'est la logique des *guerres hybrides* et la dialectique ami|adversaire ; le règne de la *dislocation*. L'échiquier choisi est celui du *jeu d'échecs* où les différentes ressources de l'État sont combinées à l'instar des pièces de ce jeu de stratégie.

- Enfin, la *compétition* boucle le triptyque d'un système où toutes les composantes sont en interaction si ce n'est en synergie permanente. L'échiquier est le *qípán* du jeu de Go, « *dont le but n'est ni de détruire les pièces adverses, ni de disloquer leur organisation, mais de les priver de leur liberté d'action en menant la "guerre par le milieu social" (GMS)*.[442] » C'est la logique de la guerre économique systémique où il s'agit de modeler l'adversaire par des manœuvres d'encerclement cognitif. On est face à une dialectique ami|allié/adversaire et au règne du *façonnement*, plus haut degré d'influence dans la fabrique du consentement proactif.

*Nationale*, Compte rendu n°68, pp. 5-6 (https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def2021068_compte-rendu.pdf) et de son interprétation par Raphaël Chauvancy (https://atlantico.fr/article/decryptage/it-s-the-strategy-stupid--le-nouvel-ordre-strategique-au-prisme-de-la-crise-ukrainienne-guerre-en-ukraine-russie-etats-unis-chine-otan-raphael-chauvancy)

[441] Raphaël Chauvancy, atlantico.fr, *op. cit.*, consulté le 16/08/2023.

[442] Raphaël Chauvancy, *ibid.* Le concept est emprunté à celui de la *political warfare* britannique.

La guerre est donc *hors limites* « *et il n'existe plus de domaine qui ne puisse servir la guerre et presque plus de domaines qui ne présentent l'aspect offensif de la guerre. Désormais ces différents espaces s'interpénètrent.* [...] *Le monde entier s'est transformé en champ de bataille au sens large*.[443] » Or, la guerre informationnelle ou *infoguerre* est bien le point nodal de la conflictualité systémique. Et cette conflictualité, déstabilisée par la lame de fond de la numérisation mais aussi par opportunisme tactique de dissimulation, emprunte la voie du cyber.

### **1)** Un champ de bataille informationnel *augmenté* par le cyberespace

Le cyber, ça sert, *d'abord*, à faire la guerre, dès lors qu'on s'inscrit dans l'approche de la guerre systémique. Si l'on suit la proposition de Bertrand Boyer d'aborder le cyberespace comme un territoire éthologique[444], le cyber est bien un théâtre d'affrontement basé sur une compétition entre acteurs individualisés. Cette confrontation établit une anarchie – hiérarchie informelle et opaque – sur des espaces mouvants séparés plus par des lignes de force éphémères que des frontières intangibles. Évoquant le conflit en Ukraine, le général Marc Watin-Augouard précise :

> « *Est-ce qu'une cyberguerre est possible ? Pour moi, c'est non dans le contexte actuel. En revanche, ce qui est vrai, c'est qu'on a le cyber dans la guerre. Et c'est deux choses complètement différentes. La difficulté, est qu'on ne sait pas à quel moment on sort du champ de la cybercriminalité pour rentrer dans le champ de la guerre, du conflit. À quel moment la cyberattaque atteint un niveau tel que ce n'est plus de la cybercriminalité classique, qu'on n'est plus dans le droit commun du code pénal mais dans le droit des conflits armés et de la Convention de Genève.* [...] *On ne gagne pas la guerre grâce au cyber. En revanche, on peut la perdre à cause du cyber*.[445] »

En réalité, la cyberguerre aura peut-être lieu. Cette conflictualité numérique n'est vraisemblablement pas arrivée à maturité comme l'avance Nicolas Mazzucchi[446]. C'est un fait, la notion de *cybercriminalité* semblerait plus indiquée pour désigner la grande majorité des cyberattaques et au regard de leurs effets somme toute limités. Comme *malwares* privilégiés dans ces offensives contre des acteurs de taille généralement modeste, les *ransomwares* et *spywares* s'en prennent avant tout aux capacités financières des entreprises par le verrouillage ou le vol de leurs données. Il est vrai par ailleurs que les médias dramatisent souvent les cas

[443] Qiao Liang & Wang Xiangsui, *La guerre hors limites*, Payot & Rivages Éd., 2006, 320 p., pp. 279-300.
[444] Bertrand Boyer, *Cybertactique*, *op. cit.*, pp. 28-30.
[445] Général Marc Watin-Augouard, intervention au *Forum Sécurité & Résilience*, 31/10/2022, diffusé sur la chaine YT *We Demain* (https://www.youtube.com/watch?v=h6Ksv-Ty11o)
[446] Nicolas Mazzucchi, « La cyberconflictualité et ses évolutions, effets physiques, effets symboliques », *Revue Défense Nationale*, 2019/6 (N° 821), pp. 138-143.

publicisés et qu'il en résulte des atteintes plus symboliques et psychologiques que concrètes. À cet égard, l'imagerie autour du cyber a été largement influencée par des schémas de pensée initiaux alimentés par un « marketing de la peur » (*cyber-Pearl Harbor*, *cyber-Armageddon*…), qu'il s'agisse des États en particulier et dans une moindre mesure des organisations privées. On parle ainsi de pouvoir égalisateur du cyber (faible|fort), autorisant par leur activisme des acteurs asymétriques sinon de vaincre du moins déstabiliser des entités de stature étatique.

Or, cette égalisation non des moyens mais des atteintes d'objectifs au moins psychologiques est chose avérée. D'abord, parce que nos sociétés contemporaines reposent on l'a dit sur des fondements économiques, et qu'en la matière, la confiance – donc les ressorts psychologiques – sont déterminants. Par exemple, les atteintes à l'image/e-réputation ou un simple tweet peuvent déstabiliser une entité publique ou privée et faire dévisser un cours boursier. Il s'agit déjà là de facteurs d'instabilité notables. En l'occurrence, le cyberespace agit bien comme un domaine amplificateur de phénomènes notamment sociocognitifs (perceptuels) propres à sa couche humaine. Sans céder à des conjectures futurologiques, il est loisible de penser que l'évolution des technologies va engendrer une explosion d'attaques informationnelles et informatiques conjuguées, qui seront de plus en plus générées et pilotées par des intelligences artificielles. À ce propos, on voit déjà la révolution des *deep fakes* se dérouler et la rapide progression d'IA capables d'assister des codeurs voire programmer par elles-mêmes des solutions malicielles[447]. Au contact des entreprises depuis de nombreuses années, Karim Lamouri confie : « *Le fameux adage : "la question n'est pas de savoir si on va être attaqué, mais quand", ça fonctionne. L'attaque, tout le monde la vivra, surtout avec la montée en puissance et la maturation future de l'IA*.[448] » Par ailleurs, il faut également replacer cette évolution dans la tendance lourde de *l'informatique ubiquitaire*, dont les objets connectés (militaires, industriels et médicaux pour les plus critiques) constitueront tant l'extension matérielle qu'immatérielle de l'hyper-connectivité. De tels systèmes autonomes notamment civils sont amenés à se multiplier et potentiellement être utilisés à des fins malveillantes. Ce que l'expert en cybersécurité, Bruce Schneier, appelle – avec sarcasme ou inquiétude – « *l'Internet+* »[449] ne manquera pas d'étendre l'ombre portée du cyber sur le monde physique.

[447] Voir aussi cet article de Yannick Chatelain sur Forbes : https://www.forbes.fr/technologie/ia-offensive-et-ia-defensive-les-defis-exponentiels-de-la-cybersecurite/. L'usage de LLM (*grands modèles de langage*) s'appuyant sur des réseaux neuronaux, pour l'heure dédié à la défense, sera aussi de plus en plus consacré aux attaques.
[448] Entretien avec l'auteur, 07/07/2023.
[449] Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company, 2018, 288 p.

De fait, si le domaine cyber fait partie intégrante du champ informationnel aujourd'hui, tout porte à croire qu'il s'opérera une inversion des périmètres quand la numérité sera en passe d'être atteinte. À ce titre, ce n'est pas un hasard si des pays tout-connectés, telle l'Estonie dès 2007, ont connu des cyberattaques assez préjudiciables. Certes, il n'existe probablement pas dans le monde numérique comme ailleurs de *wunderwaffe*[450], mais la vigilance reste de mise car les « scénarios catastrophes » sont bien documentés comme l'attestent entre autres deux hackers français[451]. Balbutiante, encore à ses débuts et vraisemblablement toujours en « phase de tests », la conflictualité numérique pourrait plus vite que prévu changer de dimension et de braqué. Tentons dès lors d'approfondir la notion de cyberguerre pour trancher le débat autour de sa réalité.

### **2)** Caractérisation de la conflictualité liée au cyberespace

Comment qualifier au mieux cette conflictualité ? Nous avons vu qu'elle a fait l'objet de nombreuses tentatives de définition : « conflictualité numérique », « cyber-conflit », « guerre numérique[452] », « netguerre », etc. On peut déjà avancer que la sanctuarisation des territoires caractéristiques du milieu physique (terrestre) n'est pas admise en milieu cyber. Ce qui en fait un objet global d'abstraction et un ensemble réticulaire ubiquitaire rétif à toute appropriation. Toutefois, on peut altérer et ainsi avoir un impact sur cet espace, physiquement, logiquement ou cognitivement. Passons alors en revue succinctement ses différentes composantes, définies communément et faute de mieux en trois couches dimensionnelles.

- ***Cyberguerre et couche physique* :** elle consiste d'abord à neutraliser les infrastructures matérielles adverses en les détruisant : câbles de transmission de communications, IXP (*Internet exchange points*), équipements informatiques, centres d'approvisionnement électrique, stations d'atterrage… On est dans le domaine du sabotage. Par ailleurs, on peut espionner (sondes) les câbles ainsi que les réseaux informatiques (cartographie-topologie) acheminant les données binaires. C'est le

[450] Expression allemande désignant des « armes-miracles » censées révolutionner la guerre.
[451] Interview de Brice Augras et Victor Poucheret, chaine *Thinkerview*, *op. cit.* Citons notamment le ransomware Wannacry qui touche, en mai 2017, près de 300 000 ordinateurs de dizaines d'entreprises dans 150 pays grâce à une faille baptisée EternalBlue de l'OS Windows XP ; ou encore le *wiper* NotPetya en juin de la même année qui aura un impact massif sur l'informatique maritime (Maersk) et engendrera notamment la perte de plusieurs milliers de tonnes de céréales. Voir notamment Andy Greenberg, « The untold story of NotPetya, the most devastating cyberattack in history », *Wired*, 22 août 2018. Par ailleurs, la Revue stratégique de cyberdéfense 2018 abonde dans ce sens en parlant de possibles cyberattaques « *de grande ampleur* […] *dont les conséquences* […] *pourraient désormais être critiques pour la Nation*. » (http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf, p. 135)
[452] Bertrand Boyer, *Cyberstratégie…*, *op. cit.*, *passim*.

domaine de l'espionnage (ou le renseignement encadré par le droit). Ces activités relèvent plus généralement de la sphère militaire avec usage d'armes numériques (logicielles) et conventionnelles (section de câbles, explosion d'une station…). Prenons l'exemple des menaces de navires russes mouillant au-dessus de nœuds de câbles en mer baltique. Les infrastructures sont construites et gérées par des acteurs privés du monde civil.


**Figure 25 :** *Cartographie des câbles sous-marins, vecteurs de 97% des communications électroniques intercontinentales*

Source : https://www.monde-diplomatique.fr/cartes/cables-sous-marins

- ***Cyberguerre et couche logique* :** elle consiste à exploiter des vulnérabilités par le biais de logiciels ou scripts malveillants. C'est le domaine des hackers/pirates informatiques par excellence car cela exige des compétences techniques plus ou moins élevées, en fonction des niveaux d'expertise en programmation notamment. Il existe trois principaux types d'attaques : *web* (basées sur les opérations d'énumération et les injections), *système* (basées sur l'usage de maliciels et le *cracking*) et *réseau* (basées sur l'emploi du *cracking* et le déploiement de charges utiles), comme le montre le schéma ci-dessous.

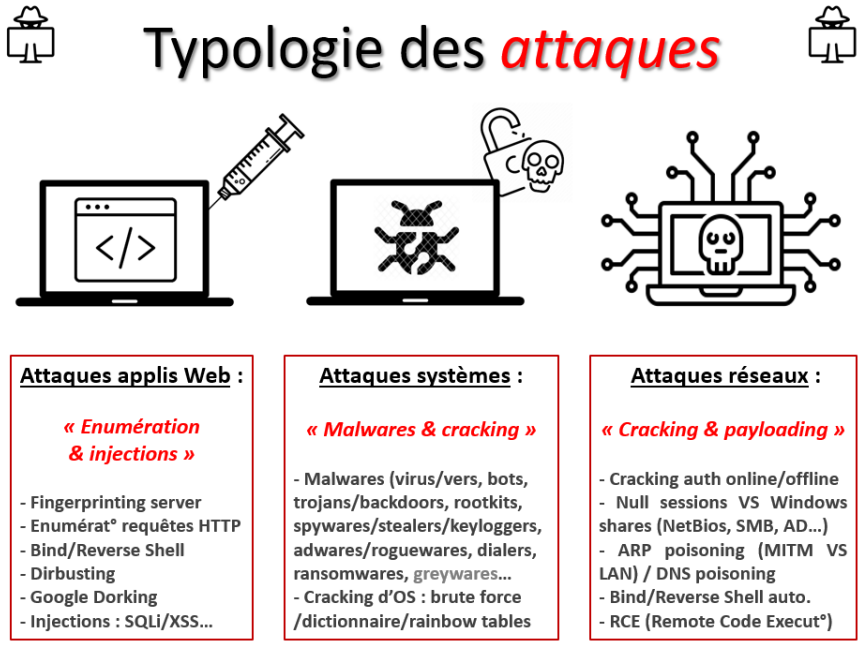



**Figure 26 :** *Typologie des principales ressources numériques visées par les hackers pour compromettre un SI*

Source : Yannick Pech, 2023. Basé sur des connaissances acquises et la pratique du *pentesting*.

Le *pentesting* est une des déclinaisons du hacking et peut être pratiqué tant par des hackers éthiques que des pirates informatiques. Il consiste à opérer des tests d'intrusion (pénétration des ressources numériques de la cible) sur les trois briques : web, système, réseau. Le cycle du *pentesting* repose sur une série d'actions que l'on peut résumer à quatre étapes : reconnaissance/OSINT ; cartographie et exploitation ; maintien d'accès et latéralisation ; obfuscation/effacement des traces.

- Les actions *d'énumération* ont pour but de cartographier l'ensemble des actifs et ressources technologiques d'un SI. Par exemple, on inventorie les différents répertoires et dossiers et ainsi l'arborescence d'un site web ou d'une base de données.
- Les *injections* consistent à insérer du code ou des scripts malveillants dans des bases de données, des champs de formulaires de pages web, etc. On peut de cette manière prendre le contrôle de telles ressources.
- Les *malwares* sont utilisés comme armes numériques, des agents dotés d'une charge utile qui va exploiter une faille logicielle dans un SI. Ils sont initialement programmés par des spécialistes mais peuvent ensuite être vendus sur étagère à des non experts.

- Le *cracking* est l'activité spécifique au forçage des dispositifs d'authentification. Des outils dédiés en facilitent le déploiement en automatisant les tâches de tentatives d'accès frauduleux.
- Le *payloading* consiste à utiliser des scripts créés *ex-nihilo* ou préétablis pour exécuter du code malveillant à distance à même de prendre le contrôle d'un terminal, d'un actif, d'un système. Et très souvent à maintenir un accès non autorisé à ces derniers en vue d'opérations futures (*backdoor*, *reverse shell*[453]).
- S'agissant des modalités techniques de recherche de vulnérabilités logiques, les pentesters utilisent des outils sur mesure (codés) ou de « prêt-à-hacker[454] » (sur étagère) pour procéder à des techniques manuelles (tests de requêtes sur différents protocoles et vérifications du comportement d'une application), semi-automatiques (ex. : suite logicielle *Burp Suite*[455]) ou automatiques (ex. : scanner de vulnérabilités *Nessus*[456]). Des systèmes d'exploitation sont spécialisés dans l'agrégation de tels outils – souvent gratuits, libres et open source –, comme les célèbres distributions Linux *Parrot Security* et *Kali Linux*[457].

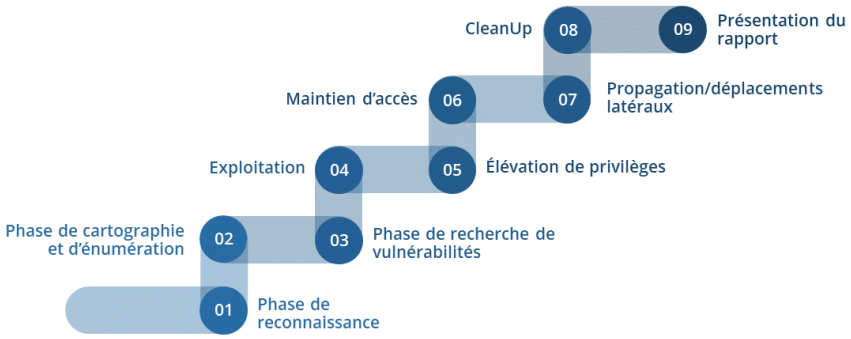



**Figure 27 :** *Méthodologie du pentesting, ici déclinée en neuf phases*

Source : https://www.login-securite.com/2019/02/22/le-pentest-de-a-a-z-methodologie-et-bonnes-pratiques-pour-securiser-son-si/. (La phase zéro serait – pour du hacking éthique bien sûr – le contrat client formalisant ses besoins).

[453] Les *shells* (interfaces systèmes/coquilles logicielles) sont des programmes (interpréteurs de commandes) à travers lesquels un utilisateur peut donner des instructions au système d'exploitation qui les exécutera. Un *reverse shell* (inversé) permet en substance d'établir un canal distant avec une machine cible sur laquelle on peut dès lors faire exécuter des commandes.
[454] On parle parfois de CaaS (*Crimeware as a Service*) quand leur exploitation vise des fins illégales.
[455] https://portswigger.net/burp
[456] https://fr.tenable.com/products/nessus
[457] https://www.parrotsec.org/ ; https://www.kali.org/

L'impact économique, réputationnel voire fonctionnel engendré par l'exploitation réussie de ces failles de sécurité peut être très élevé. C'est également au niveau de cette couche que se posent les enjeux de la gouvernance du cyberespace et en particulier de l'Internet (UIT, ICANN, W3C…)

- ***Cyberguerre et couche socio-cognitive* :** elle consiste à altérer les perceptions et représentations des foules, des individus et des organisations au sens large. C'est le règne du contenu sémantique qui, par l'union qu'il opère entre le socio-relationnel et le cognitif, s'apparente au lieu adéquat pour la manipulation psychologique. C'est le domaine qui unifie le plus mais pas exclusivement les sphères militaire et civile, publique et privée. Il s'agit probablement de la couche la plus performative en termes d'attentes et de résultats sur les environnements sociétal et économique, d'emprise par la démultiplication des effets qu'elle opère sur les biais cognitifs. On y déploie donc des techniques d'ingénierie sociale, des campagnes de propagande et de désinformation, des opérations de subversion…

Le cyber se distingue ainsi par l'entremêlement artificiel de trois couches interdépendantes que l'on peut schématiser par le continuum *câble–code–psyché*. Si chaque couche peut être altérée à son seul niveau, la combinaison d'attaques simultanées sur les trois donne les meilleurs résultats. Des atteintes aux deux premières traduiront des actes illégaux, tandis que la couche sémantique est bien sûr plus ambivalente car largement corrélée au droit à la liberté d'expression ; il est difficile de l'encadrer juridiquement. Cette nature floue et complexe est inhérente au cyber et autorise donc des actions souterraines ou sournoises, à la charnière entre secret et transparence et dans une logique tout à fait hybride.

Finalement, l'esprit qui y préside ou y sied est celui de la *maskirovka* russe. Les jeux et manœuvres conduites dans le cyber relèvent très largement des trois D de ladite doctrine soviétique : *duperie*, *déni*, *dissimulation*. D'où probablement une difficulté à vraiment consacrer l'expression de cyberguerre. Revenons donc à notre proposition initiale et infléchie de « cyberguérilla ».

### 3) Des guerres de l'information

La guérilla est définie par le dictionnaire *Larousse* comme une « forme de guerre caractérisée par des attaques continuelles, des actions de harcèlement, d'embuscades ou de coups de main. » Le but de la guérilla est généralement politique. On peut établir ses principales caractéristiques et essayer de les transposer au cyber.

| Guérilla | Cyberguérilla |
|---|---|
| Diss/asymétrie des forces | **Asymétrie** (plutôt) et multitude des acteurs |
| Action **indirecte** et tactique | Action **(in)**directe et **tactico-stratégique** |
| Moteur politique/**idéologique** collectif | Moteur **idéologique** idiosyncratique |
| Esprit de corps ± exclusif et solidarité | **Communauté souple** ou individualité |
| **Lien** (recherché) avec la population locale | Lien individuel à une communauté évanescente |
| Organisation **souple**, ± **décentralisée** | **Organisation agile, décentralisée** |
| **Mobilité**, dispersion, **flexibilité** des forces | Volatilité, **réticularité**, **flexibilité** des acteurs |
| **Fulgurance des attaques, effet de surprise** | **Fulgurance des attaques, effet de surprise** |
| Terrain d'action ± étendu et difficile d'accès | **Terrain d'action global** et facile d'accès |
| Effet psychologique limité | Effet psychologique **efficace** |

**Figure 28 :** *Parallélisme des caractéristiques entre guérilla et cyberguérilla*

Source : Yannick Pech, 2023.

Au bilan, on peut noter des similarités et une certaine proximité entre les deux notions.

Toutefois, si convoquer la notion de cyberguérilla est intéressant et correspond à une part de réalité de la cyberconflictualité, elle peut aussi dénoter un marquage trop « militarisé » ; dans tous les cas, son usage ne s'est pas imposé. Par ailleurs, en se repositionnant sur les concepts de guerre économique et d'IE, qui placent l'information au cœur des rapports de force et des jeux d'influence, la formule « guerre(s) de l'information » s'avère pratique et simple[458]. Conforté en cela par le général Burkhard qui spécifie que « *Le champ informationnel est le théâtre d'une véritable guerre témoignant de l'importance prise par les champs immatériels*[459] », il convient d'expliquer ce que reflète cette expression en réalité duale.

[458] Nous ne nous en tiendrons toutefois pas à une définition arrêtée, et les termes cyberguerre et cyberguérilla pourront être employés, avec ou sans précision complémentaire.

[459] https://archives.defense.gouv.fr/portail/actualites2/florence-parly-presente-la-doctrine-militaire-de-lutte-informatique-d-influence.html

En premier lieu, l'infoguerre se décline en trois modalités : la *guerre pour, par et contre l'information*[460]. En second lieu, cette dernière est à appréhender à l'aune de ses deux dimensions :

**L'une, *technique-informatique***[461] :

- *Guerre pour l'information* (*espionner*) : acquisition d'informations (blanche, grise ou noire) à fin de renseignement d'intérêt cyber (RIC) ou reconnaissance/OSINT sur les éléments techniques d'une cible (topologie-réseau, vulnérabilités logicielles/système…) à fin de hacking.
- *Guerre par l'information* (*neutraliser*) : opérationnalisation de l'information à des fins d'offensive numérique-logique (logicielle).
- *Guerre contre l'information* (*sécuriser*) : mesures de sûreté des systèmes d'information ou de brouillage des systèmes informatiques adverses.

**L'autre, *immatérielle-sémantique*** :

- *Guerre pour l'information* (*renseigner*) : acquisition d'informations (blanches voire grises) pour surveiller l'adversaire, agir avant lui et maintenir une dissymétrie informationnelle.
- *Guerre par l'information* (*influencer*) : opérationnalisation de l'information à des fins d'offensive numérique-sémantique. Exploiter le capital informationnel et les connaissances pour influencer (bas niveau d'ingénierie sociale) voire modeler l'environnement concurrentiel (haut niveau d'ingénierie sociocognitive). Cela rejoint l'objectif-modalité défini par Christian Harbulot[462] : la *résonance* (optimisation des caisses de résonnances, création et exploitation de réseaux d'influence, animation de forums de discussion…)
- *Guerre contre l'information* (*aveugler*) : interdire l'accès à l'information à l'adversaire, le maintenir dans l'ignorance (*agnotologie*) en vue de le paralyser. Cela rejoint les objectifs-modalités définis par Christian Harbulot : la *tromperie* (désinformation, manipulation, discrédit…) et la *contre-information* (identification des points faibles de l'adversaire, exploitation de ses contradictions, utilisation de l'information vérifiable…)

[460] Olivier Coussi, Audrey Knauf, Nicolas Moinet, « Les guerres pour, par et contre l'information », *op. cit*.
[461] C'est l'approche traditionnelle en France, y compris dans les instances civiles. Il en va de même avec les cyberdéfense & cybersécurité qu'on aborde surtout sous l'angle technique. D'où une carence doctrinale et une consécration très tardive (2022) de l'influence (*guerre par l'information*) comme fonction stratégique malgré la plus précoce Lutte *informatique* d'influence (L2I) des Armées (2021).
[462] Christian Harbulot, *L'art de la guerre économique*, *op. cit.*

Il est pertinent sinon nécessaire de les distinguer pour les étudier car elles induisent des attaques informatiques (surtout le *pour* et le *par*) d'un côté[463], et des offensives informationnelles (surtout le *pour* et le *par*) qui se doublent d'offensives cognitives (surtout le *par* et le *contre*) de l'autre. C'est pour cette raison qu'on parle parfois de cyberguerre pour désigner la première, et de guerre informationnelle pour la seconde. Elles ont toutefois tendance à s'hybrider ou plutôt se combiner puisque les contenants/véhicules de l'information sont communs aux deux. Par ailleurs, on note la coïncidence entre le triptyque du général Burkhard et la tripartition typologique des hackers :

- *compétition* : hackers blancs (éthiques) ;
- *contestation* : hackers gris (hacktivistes) ;
- *affrontement* : hackers noirs (criminels).

Après avoir précisé le rôle démultiplicateur de la conflictualité tenu par le cyber et décliné ses caractéristiques martiales, nous proposons d'illustrer le rôle prééminent que joue désormais le hacking dans cette guérilla informatique et informationnelle à travers l'étude de trois cas convoquant une triple grille d'analyse. Précisément, les hackers sont les profils les plus aptes à maîtriser les deux versants de la guerre de l'information. Si celle-ci s'apparente à une cyberguérilla, alors le hacking en constitue probablement le fer de lance, placé dans une zone grise à l'intersection entre légalité et illégalité.

[463] L'expression « guerre informatique » a été employée officiellement par le rapport Romani en 2008 pour désigner le triptyque de cette guerre de « l'information technique » (https://www.senat.fr/rap/r07-449/r07-449.html, consulté le 15/08/2023.

## **B.** *Le hacking comme opération spéciale permanente des guerres de l'information*

« *Une fois, est un hasard.*
*Deux fois, est une coïncidence.*
*Trois fois, est une action ennemie.* »

Ian Fleming (*Goldfinger*)

*Confidentialité, intégrité, disponibilité* : tel est le triptyque d'airain de la cybersécurité.

Face à cette posture de sûreté des systèmes d'information (SI), le hacking, *lato sensu* : ensemble des techniques de détournement d'usage de dispositifs de tous ordres. On « hacke » des systèmes, des ordinateurs, des logiciels, la pensée, les foules. On parle de hackers éthiques, d'hacktivistes, de hackers noirs. Cette plasticité sémantique, bien qu'en partie liée à des effets mémétiques (*growth hacking*, *hackatons*…), illustre l'hybridation de pratiques dont la ligne de crête entre légalité et illégalité est de plus en plus floue.

Les cyberattaques connaissent aujourd'hui un essor exponentiel qui touche tous les acteurs et domaines : public, privé, politique, militaire, économique, social. Avec sa dimension transversale, le cyberespace unifie dans une réalité augmentée les milieux de la stratégie. Ainsi, une guerre sans limites, greffant au monde physique un méta-territoire cybernétique, abolit des cloisons établies de longue date.

Le hacking est par conséquent une composante centrale des guerres menées par, pour et contre l'information. Schématiquement séparé en trois couches, le cyberespace est en effet tout à la fois le support physique, logique et sémantique par et sur lequel vont être déployées des attaques protéiformes visant à :

- saboter, détruire, paralyser (couche matérielle, guerre contre l'information) ;
- faire de l'espionnage, pirater, altérer (couche logique, guerre pour l'information) ;
- faire du renseignement, désinformer, subvertir (couche sociocognitive, guerre par/pour/contre l'information).

Pour reprendre les mots de Guillaume Poupard au sujet de l'état de la cybermenace, nous sommes face à « *une catastrophe absolue*. » Depuis des années maintenant au fait de ces cybermenaces, comment expliquer que les acteurs politiques et économiques soient toujours victimes de tels agissements ? S'agit-il de failles et manquements spécifiquement techniques ou organisationnels ? Comment dès lors appréhender cette apparente fatalité ? Face à cette guerre par, pour et contre l'information, les pratiques de hacking ne constituent-elles pas

désormais le nœud gordien de la sécurité informationnelle dans une société omninumérique ? Dans ce sous-chapitre, nous nous attacherons à sonder le rôle du hacking dans les guerres de l'information. Pour tenter de répondre à ces questions, nous soumettrons trois cas de hacking d'organisations à une triple grille de lecture.

Du point de vue théorique, nous convoquons d'une part, la boucle OODA comme outil d'aide à la décision emprunté au monde militaire et transposé à l'intelligence économique. Cette matrice n'a jamais été appliquée à la méthodologie du hacking, du moins en France. D'autre part, nous inscrivons notre analyse dans le concept de *guerre économique systémique* démocratisé par Christian Harbulot selon lequel les rapports conflictuels empruntent des voies de moins en moins militaires mais, à l'inverse, des formes plus globales[464]. Enfin, la grille de lecture de la *guerre réseau-centrique*, issue du débat sur la *Révolution dans les affaires militaires*, vient compléter notre approche.

D'un point de vue méthodologique, notre investigation se fonde sur l'exploitation de sources secondaires (presse, analyses spécialisées, témoignages de hackers). Le premier cas considère l'étude d'une opération de sabotage qui a mis aux prises un acteur présumé étatique et une compagnie pétrolière (couche matérielle). L'autre apporte un éclairage sur le piratage massif de SolarWinds et ses dizaines de milliers de clients politiques et économiques, sur la base d'une altération de son logiciel Orion (couche logique). Enfin, un troisième cas traite des manœuvres de guerre psychologique et notamment l'*astroturfing* mises en œuvre dans l'affaire Cambridge Analytica (couche sociocognitive).

Cet appareillage théorico-empirique nous permettra de sonder l'hypothèse d'un phénomène de hacking comme levier essentiel voire pierre angulaire de la guerre de l'information.

### 1) Un triple cadre analytique : boucle OODA, combat réseau-centrique, guerre économique systémique

Nous proposons un cadre théorique fondé sur la mutualisation de trois grilles de lecture. D'abord, le modèle OODA a comme bon nombre de théories militaires été appliqué au monde civil, notamment dans la recherche en intelligence économique[465]. Il peut s'articuler avec la doctrine du *combat infocentré* qui repose sur l'idée d'une guerre en réseaux temps-réel. Enfin, le concept de guerre économique plante le décor contextuel où l'information devient le point

[464] Christian Harbulot, « Chine/Etats-Unis ? Sortie de crise ? La guerre économique systémique comme grille de décryptage », *Communication & Influence*, n°111, 2020, pp. 1-6.
[465] Nicolas Moinet, « Le renseignement au prisme du couple agilité-paralysie », *Prospective et stratégie*, 2019/1 (n°10), pp. 13-27.

nodal d'un système qu'il s'agit de contrôler à des fins de puissance et d'influence. Or, le hacking est un outil de maîtrise de l'information, qu'il s'agisse d'y avoir accès, de la manipuler ou la dissimuler.

### a) *La boucle OODA ou le décryptage des modèles de conflits*

En 1976, John Boyd, ancien pilote de combat de l'USAF, publie *Destruction & Creation* où il expose le fruit de ses travaux de stratégiste-tacticien et en particulier sa théorie pratique de boucle OODA. Fondée sur son expérience de la manœuvre aérienne, cette méthode d'analyse repose sur la maîtrise de la prise de décision en temps contraint. Quatre processus continus sont donc mis en œuvre dans un cycle voulu court et harmonieux chez soi et à l'inverse long et chaotique chez l'adversaire : Observation-Orientation-Décision-Action. Cette confrontation donne la prime à l'attaquant qui, par une série d'initiatives agiles, paralysera l'adversaire noyé sous les manœuvres et incapable de riposter efficacement. John Boyd développera son approche pour en faire une théorie générale sur le *decision-making* transposée au monde économique[466].

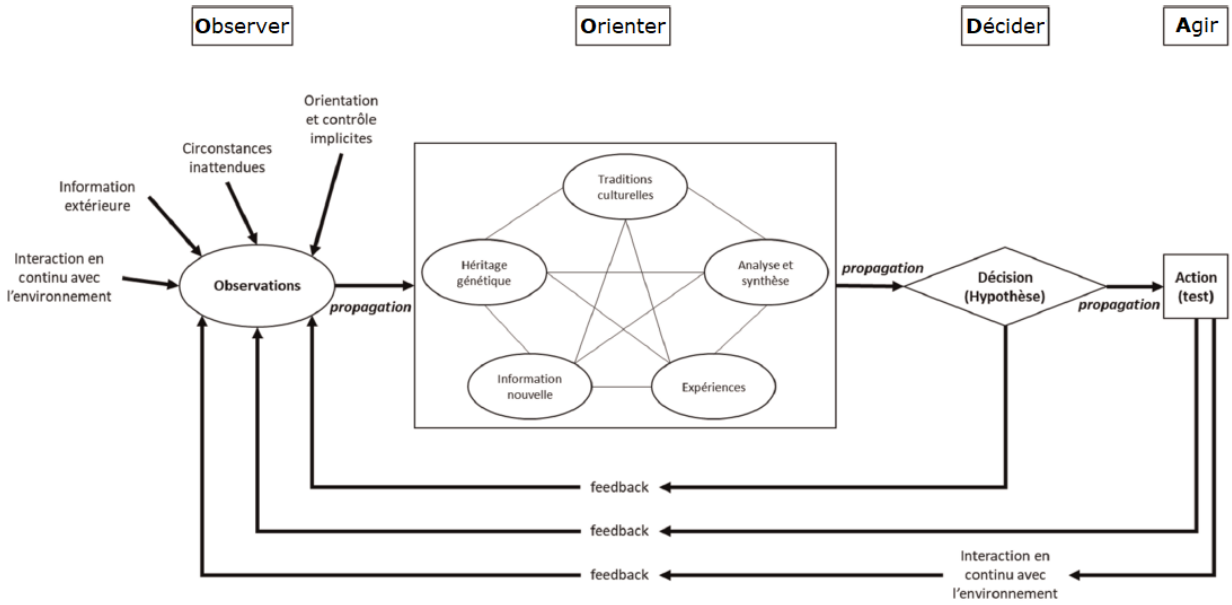



**Figure 29 :** *La boucle OODA*[467]

Ainsi, sur fond de compétition généralisée, John Boyd décompose sa matrice en focalisant l'attention sur la phase d'orientation. Là entre en ligne de compte le double

[466] Olivier Coussi & Nicolas Moinet, « Extension du domaine de la prédation. La vente d'Alstom à General Electric», *Revue française de gestion*, 2019/8 (n°285), pp. 211-227.
[467] John R. Boyd, *Destruction and Creation*, USCGSC, KS, 1976.

processus de destruction (analyse) et création (synthèse) : en fonction de son expérience, de son héritage biologique ou de ses différents tropismes culturels, tout acteur façonne des images mentales lui permettant d'appréhender l'environnement conflictuel. Notre manière d'observer, nos décisions et actions sont ainsi conditionnées par ces schémas cognitifs, qu'un antagoniste agile parviendra à analyser, critiquer, reconstruire et enrichir pour éclairer d'une lumière neuve sa tactique-stratégie. Du reste, il est pertinent d'envisager d'y insérer un niveau opératique comme le propose opportunément Stéphane Goria[468]. Ce faisant, il pourra entretenir le maximum de stabilité dans son camp (*dispositif intelligent*) et, par ses manœuvres d'influence sur les images mentales de son rival, générer le désordre dans le camp adverse (*dispositif perturbé*).

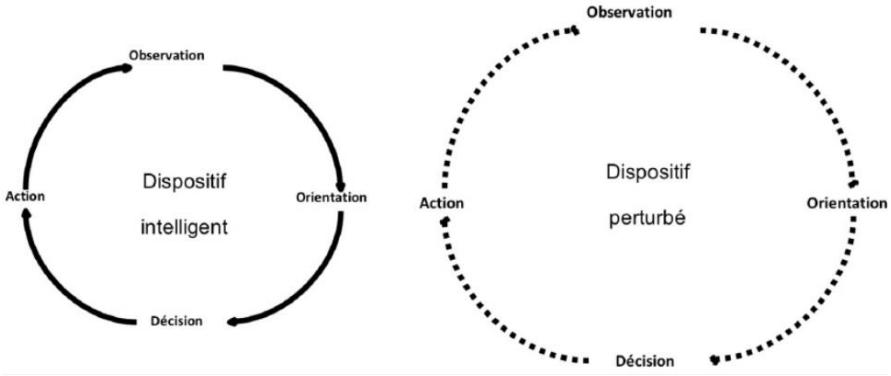



**Figure 30 :** *La relativité des boucles OODA*[469]

Dans le contexte de la guerre informationnelle, le hacking complexifie la donne. Car les quatre processus itératifs du cycle s'inscrivent dans un espace-temps hyper-contraint où les actions sont furtives – sans être forcément opaques – et fulgurantes. En soi, les cyberattaques constituent désormais autant de *cygnes noirs*[470] puisque, comme le disent les experts en cybersécurité et le reconnaissent eux-mêmes certains acteurs économiques, la question n'est pas de savoir « si on va être attaqué, mais quand ? » Le cas des *Advanced Persistent Threats* (APT*) montre de manière éclairante combien il est difficile de faire face à ces agressions. Les APT sont des hackers-corsaires sponsorisés par des structures étatiques et menant des opérations méticuleuses et itératives au moyen de malwares et *exploits* sophistiqués élaborés

[468] Stéphane Goria, « L'utilité de l'échelle opératique pour considérer des stratégies d'intelligence et de guerre économique », *Revue internationale d'intelligence économique*, 2021/2 (Vol. 13), pp. 43-60, pp. 49-50.
[469] Nicolas Moinet, « Le renseignement au prisme du couple agilité-paralysie », *op. cit.*, p. 18.
[470] Nassim N. Taleb, *Le cygne noir : La puissance de l'imprévisible*, Les Belles Lettres, 2008, 496 p. Un *cygne noir* est un évènement aléatoire tout à fait improbable *a priori*. Pourtant, son explication rationnelle devient évidente *a posteriori*, à l'image des premiers cygnes de couleur noire que les Européens rencontrent en Océanie au XVIII[e] siècle, alors qu'ils avaient toujours pensé qu'ils étaient blancs en tout lieu et tout temps, comme sur leur propre continent.

sur mesure et à usage unique[471]. Notre réflexion nous amène à considérer l'utilité du paradigme réseau-centrique pour replacer le hacking dans sa matrice techn(olog)ique.

### b) *La guerre en réseau ou le combat info-centré*

La *Network Centric Warfare* est un concept né Outre-Atlantique d'un processus réflexif qui atteint sa maturité à la fin des années 1980. L'âge de l'information pose le défi global de la numérisation au monde militaire, qui réfléchit à l'opportunité d'intégrer le *réseau des réseaux* dans sa chaine opérationnelle et de commandement. La fin : atteindre la *supériorité informationnelle* ; le moyen : fusionner les différentes strates du champ de bataille (capteurs-décideurs-acteurs). Strates dont il est aisé de trouver les homologues dans le monde civil. Ainsi, à la mise en réseau du champ de bataille répond la numérisation de la société et la réticularité offerte par l'Internet ou le Web social.

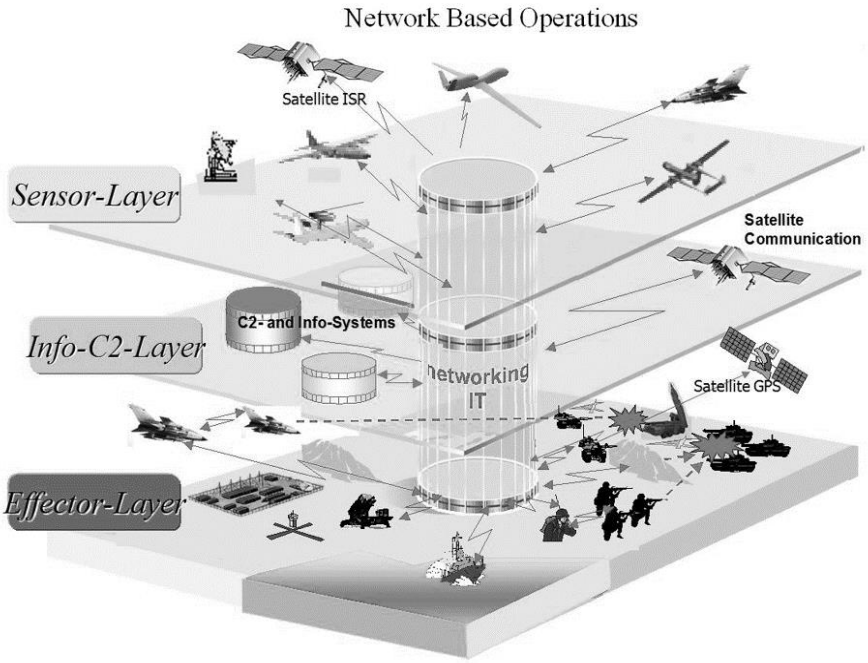



**Figure 31 :** *Représentation du concept de guerre réseau-centrique*[472]

S'il a le mérite de présenter clairement le concept notamment sur le plan des opérations militaires, le schéma ne reflète toutefois pas les enjeux et défis posés par « l'intelligence ambiante » ou *informatique ubiquitaire*, dans le domaine militaire comme civil en particulier

[471] L'acronyme signifie à la fois les actions (le type d'attaques sophistiquées) et leurs auteurs (hackers-corsaires).
[472] Kevin Benedict, *Enterprise Mobility, Netcentric Operations and Military Mobility*, 24 août 2011 (https://mobileenterprisestrategies.blogspot.com/2011/08/enterprise-mobility-netcentric.html) et Christopher Richardson, *Bridging the air gap: an information assurance perspective*, thèse de doctorat en science physique et ingénierie, université de Southampton, 2012.

avec les objets connectés[473]. Ainsi, cette intégration de systèmes informatiques communicants, de plus en plus autonomes (intelligence artificielle[474]), dans les lieux et objets du quotidien surajoute une couche de capteurs à un niveau « urbi-centré » (*smart cities*, domotique…) et surtout individu-centré, qui redéfinit les approches et révolutionne le modèle du hacking. Cet environnement holo-connecté qui, selon la CNIL, menace de se diriger vers le transhumanisme voire le post-humanisme[475], ouvre ainsi des perspectives nouvelles dans « l'infovalorisation » – appliquée au hacking –, conçue comme l'exploitation optimale des ressources informationnelles que permettent les nouvelles technologies. *In fine*, le hacking pourra viser directement les personnes physiques si leur corps est de plus en plus « augmenté ».

Sur un plan plus global, la colonne vertébrale de la NCW repose sur une *Global Information Grid* (GIG) qui peut être assimilée à un *échiquier invisible* matriciel, dont les trois strates rappellent les couches cyber. Si l'information est le nerf de la guerre, détenir la suprématie informationnelle permet donc de la gagner et consiste à maîtriser la technique et la technologie, *le médium e(s)t le message* (McLuhan), contenant & contenu. La syntaxe qui sous-tend l'édification technique de l'industrie 4.0 fait écho à la sémantique du discours technologique. Dans le monde militaire comme civil, cette course à la supériorité informationnelle est poursuivie de longue date par les États-Unis. Or, le nerf de la conflictualité, c'est plus que jamais l'économie et son corollaire l'innovation techn(olog)ique. La compétition s'inscrit dès lors dans la matrice d'une guerre économique comme poursuite de la puissance par d'autres moyens.

### c) *La guerre économique systémique ou l'art du piégeage cognitif*

« *Mode de domination qui évite de recourir à l'usage de la puissance militaire pour imposer une suprématie durable* »[476], la guerre économique systémique postule que l'économie mondialisée a converti en système le théâtre des rapports de force internationaux que gouvernent les impératifs monétaires, commerciaux et financiers. Les postures théorisées respectivement dans *La guerre hors limites*[477] et la doctrine de la « guerre nouvelle génération » du général Gerasimov en 2014, sont la preuve par l'action des versants russe et chinois de la *guerre hybride* américaine. La guerre doit être comprise tel un phénomène

[473] Paula Fraga-Lamas, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo, Miguel González-López, « A review on internet of things for defense and public safety », *Sensors*, 16(10), 2016, 1644 p.
[474] Seyed M. Ghaffarian & Homayoun R. Shahriari, « Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey », ACM Computing Surveys (CSUR), 50(4), 2017, pp. 1-36.
[475] https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf
[476] Christian Harbulot, « Chine/Etats-Unis ? Sortie de crise ? La guerre économique systémique comme grille de décryptage », *op. cit.*, p. 2.
[477] Qiao Liang & Wang Xiangsui, *La guerre hors limites*, *op. cit*.

éminemment systémique, sans limites, et dont la traditionnelle dichotomie des temps de paix et de guerre ne fait plus sens.

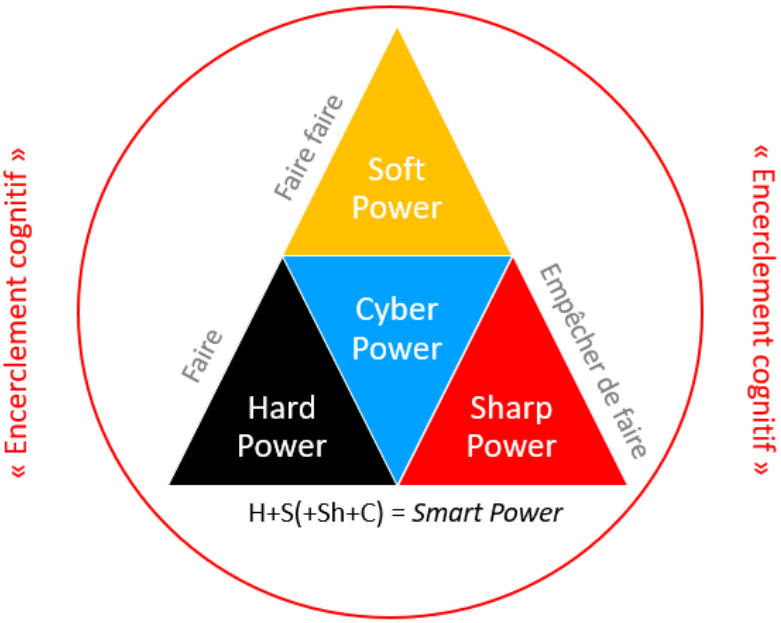



**Figure 32 :** *Les modalités de la puissance dans le cadre de la guerre systémique*

Source : Yannick Pech, 2023.

On l'a dit, la clé de voûte de cette guerre est le *Soft Power*. Tous les États aujourd'hui se conforment – ou feignent de consentir – à un ensemble de normes supranationales pour éviter le recours à la violence en usant de moyens supposés pacifistes et transparents, sur fond de mystification morale. Par-delà la question du *qui* prescrit la norme, c'est celle du *qui* la manipule selon ses intérêts, dans une logique d'*encerclement cognitif* de ses adversaires. La stratégie consiste dès lors à soumettre la volonté de l'autre à la sienne, mais plus militairement: tutelle financière, normes juridiques, influence culturelle, formatage des élites à une pensée dominante, etc.

Les acteurs de la guerre systémique sont amenés à exploiter les multiples facettes de la lutte informationnelle, mutualisant *Soft, Hard, Sharp et finalement Cyber Power*. Prolongement numérique de la diplomatie coercitive, citons la *cybercoercition* qui consiste à user ou menacer de recourir à des cyberattaques en vue d'imposer son agenda géostratégique[478]. Elle porte en germes la banalisation des opérations de hacking et de *hack back*, que les puissances occidentales invoquent désormais en guise de légitime défense pour

[478] https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html.

une « juste » (cyber)guerre. En outre, le cyber tend à unifier les trois autres formes de puissance. Ainsi, la guerre systémique nécessite une conjonction des modes de puissance. Là se situe peut-être la véritable signification d'un *Smart* Power.

### **2)** Un triple cas méthodologique : Triton, SolarWinds, Cambridge Analytica

Ces grilles de lecture seront appliquées sur trois cas présentés ici. Emblématiques de leur domaine respectif, ces affaires ont été retenues pour leur impact psychologique et leur nature archétypale des rapports de force informationnels à venir. La méthodologie convoquée se fonde sur des techniques d'analyse qualitative et l'exploitation de sources secondaires. En dépit des difficultés liées à l'étude du hacking, le rapprochement de différents types de sources telles que la presse (vulgarisation), des organismes de recherche (analyse), et les témoignages de hackers éthiques (expertise) confère un bon degré de fiabilité. L'étude s'adosse à un corpus susceptible de tester notre hypothèse par l'usage d'une supra-analyse[479], puisque nous investiguons des cas qui n'ont pas été soumis à une extrapolation visant à définir précisément les rapports entre hacking et guerre informationnelle, et à inscrire celui-ci dans un dispositif théorique propre à nourrir la recherche en IE et en SIC. La première affaire est déjà singulière car elle va bien au-delà de la simple question de la maîtrise de l'information, en posant celle de l'intégrité physique même d'agents économiques.

#### **a)** ***Triton : itération de la guerre « cyber-physique »***

Attribuée à la Russie par la firme californienne FireEye, cette cyberattaque a ciblé en 2017 une usine pétrochimique appartenant à la compagnie saoudienne Petro Rabigh. Elle s'inscrit dans une série de manœuvres initiées dans les années 1980 contre des entreprises publiques du secteur de l'énergie dans plusieurs pays, comme la France avec l'espionnage d'Areva (2011)[480]. Ces mêmes États sont parfois les auteurs des attaques, à l'image des EUA et Israël à travers l'opération conjointe *Olympic Games* (2010-12) destinée au sabotage d'installations industrielles[481]. La monarchie saoudienne en particulier a fait l'objet de nombreuses intrusions informatiques lors des opérations *Night Dragon* (2011) et *Shamoon* (2012)[482].

[479] Voir le travail de Janet Heaton, *Reworking Qualitative Data*, Sage Publications, 2004, 160 p.
[480] https://www.lexpress.fr/economie/entreprises/areva-victime-d-une-attaque-informatique-de-grande-ampleur_1364967.html
[481] Gabrielle Desarnaud, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Études de l'Ifri*, janvier 2017. La sous-opération « Stuxnet », fondée sur l'élaboration conjointe d'un ver informatique éponyme attribué à la NSA et l'unité 8.200 de *Tsahal*, inaugura les attaques cyber-physiques dans lesquelles on peut ranger Triton.
[482] *Night Dragon* est le nom générique de plusieurs attaques de cyber-espionnage ayant touché 71 organisations dont l'ONU et le Comité international olympique. *Shamoon* est un virus informatique qui a notamment touché

La plupart de ces attaques ont visé des actifs informatiques pour faire de l'espionnage. Bien qu'il marche dans le sillage de ces opérations, le cas Triton est assez singulier car considéré comme une opération de sabotage ciblant spécifiquement les systèmes instrumentés de sécurité (SIS) des systèmes de contrôle industriel (SCADA). On peut en apprécier la topologie réticulaire.

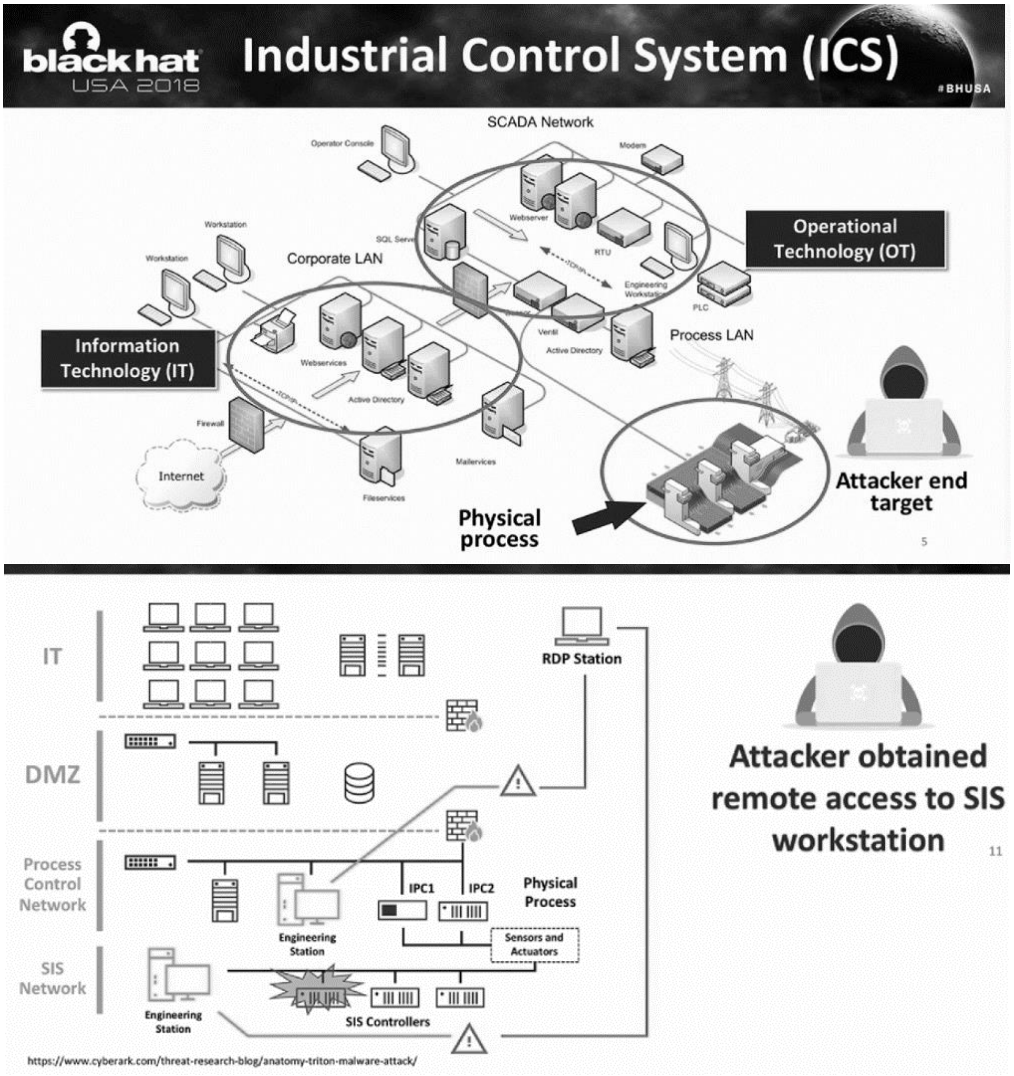



**Figure 33 :** *Topologie type du réseau physico-logique ciblé | vecteur d'attaque Triton*[483]

Un document issu d'une conférence Black Hat, parmi les évènements mondiaux qui font autorité dans le domaine du hacking, décrypte le *modus operandi* de cette attaque

des dizaines de milliers d'ordinateurs des entreprises saoudienne Aramco et qatarie RasGas. Voir notamment Danilo D'élia, « La guerre économique à l'ère du cyberespace », *Hérodote*, 2014/1-2 (n° 152-153), pp. 240-260.

[483] Andrea Carcano, Younes Dragoni, Marina Krotofil, *How TRITON Disrupted Safety Systems & Changed the Threat Landscape of Industrial Control Systems*, conférence Black Hat USA 2018.

expérimentale qui se révélera en définitive infructueuse[484]. Les SIS reposent sur des logiciels qui pilotent des éléments électromécaniques comme des valves ou des clapets. Leur objectif consiste à gérer l'équilibre des systèmes automatisés (homéostasie), la pression d'un carburant ou encore la température d'un liquide, en somme garantir une maitrise de seuils prévus et neutraliser tout dysfonctionnement pouvant mener à un accident industriel. Triton a donc été pensé et programmé pour attaquer l'articulation entre le domaine numérique et les matériels mécaniques. C'est de ce constat que les auteurs ont classé Triton dans la guerre hybride « cyber-physique », entre conflictualités cinétique (destruction des masses matérielles) et non cinétique (altération immatérielle, logicielle, informationnelle). D'autres attaques se concentrent surtout sur les éléments logiciels de la cible, comme pour SolarWinds.

### b) *SolarWinds : « Bien plus qu'un simple incident d'espionnage »*

C'est par ces mots que la Maison-Blanche qualifiera ce qui est considéré comme l'une des cyberattaques les plus sophistiquées jamais déployées. Découverte fin 2020, cette *supply chain attack* concerne la compromission d'une plateforme logicielle de gestion de réseaux informatiques baptisée Orion et distribuée par l'entreprise texane SolarWinds. Son *modus operandi* n'est pas nouveau et a déjà été utilisé par exemple en 2017 contre un éditeur commercialisant le logiciel utilitaire grand public *CCleaner*[485]. Il s'agit schématiquement de s'introduire dans les serveurs de la cible et d'y substituer une mise à jour – vérolée – à venir de son logiciel qui sera ainsi déployée sous la forme d'un cheval de Troie, lequel en liaison avec son C2 (serveur de commande & contrôle de l'attaquant) pourra activer sa charge utile de code malveillant sur les systèmes d'information cibles et attendre d'autres instructions ou modules d'attaque. En l'espèce, ce *trojan* est dénommé ironiquement « Sunburst/Solorigate », et l'attaque attribuée aux corsaires d'APT29 *alias* « Cozy Bear », un groupe lié au service de renseignement extérieur russe, le SVR.

[484] Voir aussi https://www.usinenouvelle.com/article/exclusif-le-recit-par-schneider-electric-de-triton-l-attaque-qui-a-fait-trembler-l-industrie.N1816192.
[485] https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

**ATTAQUE SUR CHAINE LOGISTIQUE**
Les attaquants injectent du code malveillant dans la bibliothèque de liens dynamiques (DLL) d'un logiciel légitime (Orion). Cette DLL compromise est distribuée aux organisations qui utilisent ledit logiciel.

**EXÉCUTION ET MAINTIEN D'ACCÈS**
La DLL compromise se charge au démarrage du logiciel, et le code malveillant active les fonctionnalités de la porte dérobée (*backdoor*).

**CONTOURNEMENT (« ÉVASION ») DES SYSTÈMES DE DÉTECTION D'INTRUSION (IDS)**
La porte dérobée procède à de nombreux contrôles automatiques pour vérifier qu'elle évolue furtivement sur un réseau compromis.

**RECONNAISSANCE**
La porte dérobée collecte des informations sur le système.

**SERVEUR INITIAL DE COMMANDE & CONTRÔLE (C2)**
La porte dérobée se connecte à un C2. Le domaine auquel il se connecte se base en partie sur l'information collectée auprès du système, rendant chaque sous-domaine unique. La porte dérobée est susceptible de recevoir l'adresse d'un autre C2 auquel se connecter.

**EXFILTRATION DE DONNÉES**
La porte dérobée transmet les informations collectées à l'attaquant.

**ATTAQUES CONDUITES MANUELLEMENT**
La porte dérobée suit les instructions de l'attaquant transmises via le C2. Le large spectre de fonctionnalités de la porte dérobée permet d'opérer d'autres manœuvres, telles que : vol d'identifiants, progressive élévation de privilèges, mouvement latéral sur le réseau de la cible.

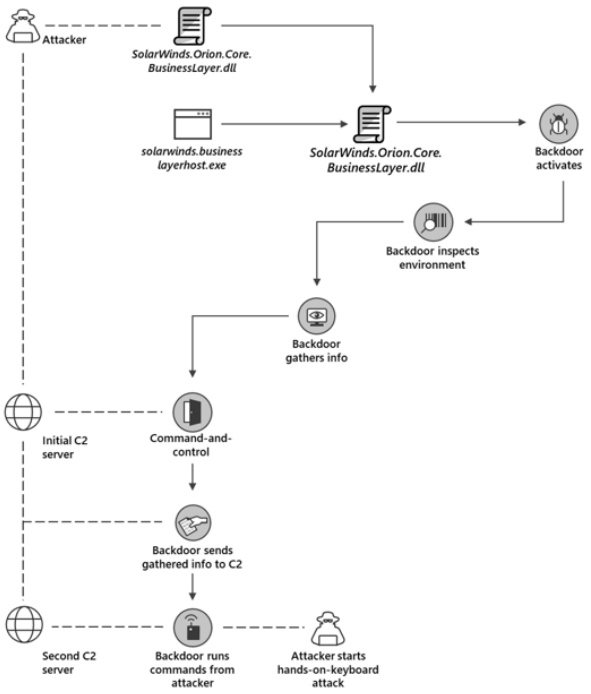



**Figure 34 :** *Modus operandi de l'attaque contre Orion/SolarWinds*[486]

Eu égard à sa sophistication et sa signature remontant à 2019, cette opération a toutes les caractéristiques d'une APT soutenue par un État. Sa portée est considérable et on en ignore encore les implications globales. Les dernières estimations tablent cependant sur près de 18.000 intranets et 400 grandes entreprises touchés, et sur de multiples usurpations d'identités, vols de données et menées d'espionnage des communications[487]. Fournisseur de nombreuses administrations états-uniennes et entreprises privées dans le monde, SolarWinds a malgré elle été le vecteur d'une attaque allant jusqu'à impacter des firmes de cybersécurité. L'attaque Sunburst comme Triton restent susceptibles d'avoir techniquement échoué mais, dans tous les cas, d'avoir réussi s'il s'agissait d'éprouver les propriétés systémiques de la cybersécurité. Jouer aux apprentis sorciers, c'est aussi le sens des manipulations de masse qui ont cours dans et via le cyberespace. Le cas Cambridge Analytica est édifiant, qui a frayé la voie.

### c) *Cambridge Analytica : cas d'école de l'astroturfing*

« *L'avenir de la politique, c'est la cyberguerre*. » Avec ces paroles de profane supposé, le philosophe Michel Onfray pourrait bien voir juste quand il évoque ici les manifestations de la guerre informationnelle qui se joue lors des campagnes électives. C'est ce qui advient pendant

[486] Source : Microsoft Threat Intelligence Center (https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/)
[487] Chaine YT Cybervox, épisode 5 (https://www.youtube.com/watch?v=Z6UmvkIbNrw).

les élections américaines de 2016. Dans le cadre d'une campagne d'*astroturfing* impliquant directement Facebook, cette société britannique d'analyse en *big data* a interféré et probablement concouru à la victoire de Donald Trump ou, en contrechamp, à la défaite d'Hillary Clinton. Fondée sur le slogan « *Les données déterminent tout ce que nous faisons* » et le but avoué « *de changer le comportement grâce aux données* », Cambridge Analytica fait écho aux *technologies persuasives* de Brian J. Fogg.

En s'attachant ses services, l'équipe de Trump souhaite influer sur le comportement de la fraction indécise du corps électoral. Pour ce faire, Cambridge Analytica peut s'appuyer sur des outils psychométriques et de traitement de données massives. Par le biais de logiciels comme *Data Models* (typologie des électeurs) et *Custom Data Manipulation* (psychographie) qui vont cartographier les centres d'intérêt, les personnalités et les orientations des publics-cibles, Cambridge Analytica va ensuite armer les algorithmes de sa plateforme *Ripon*. Nous avons des éléments probants sur cette affaire grâce à une enquête parlementaire britannique, et l'instruction d'une plainte portée par la Commission fédérale pour le commerce fondée sur les révélations du lanceur d'alerte Christopher Wylie[488]. Selon ses mots, la firme est « [une] *machine à retourner le cerveau de la guerre psychologique* […] ». Sans entrer dans les détails techniques, l'entreprise est accusée d'avoir, dans un premier temps, collecté les données de 87 millions d'usagers de Facebook via l'application *Thisisyourdigitallife* créée par un chercheur anglo-américain et proposant des quizz rémunérés à vocation scientifique. Dans un deuxième temps, la société aurait visé directement les murs sociaux individuels des utilisateurs Facebook indécis en les inondant de *ghost posts* itératifs basés sur des mèmes décrédibilisant Hillary Clinton.

[488] ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter

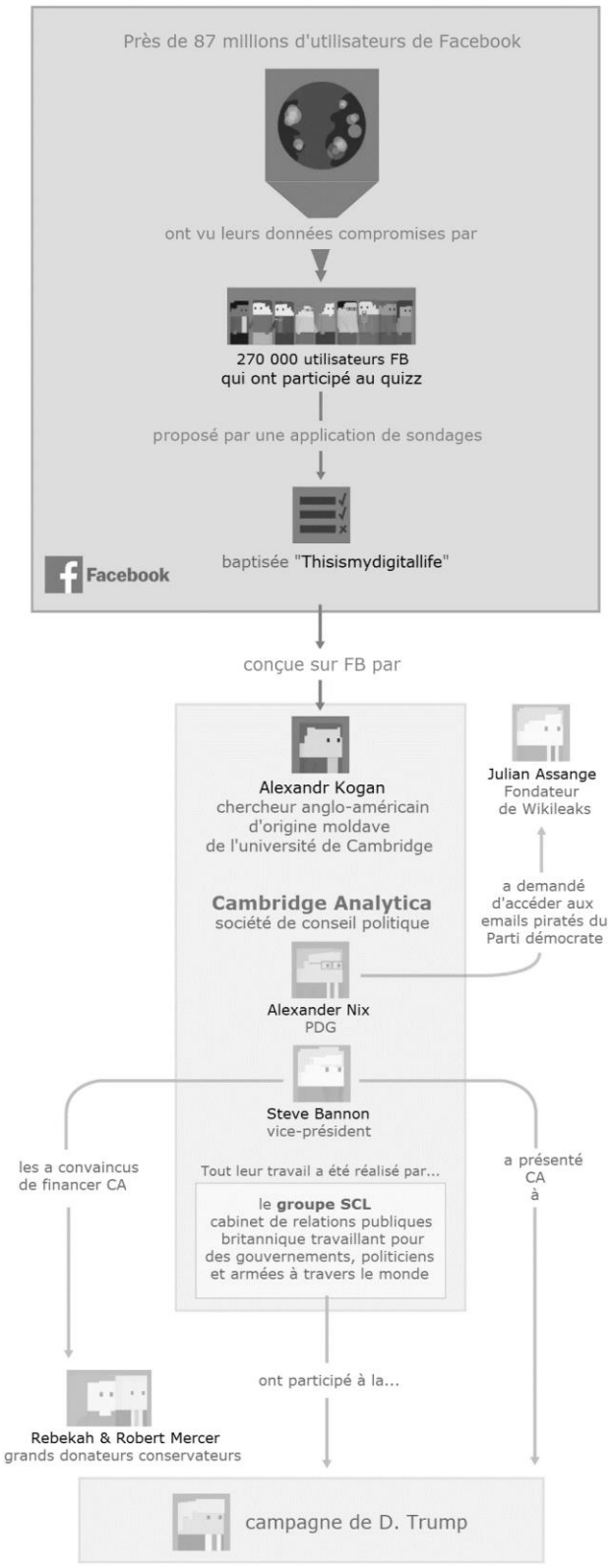



**Figure 35 :** *Déroulement de l'affaire et connexions réticulaires*[489]

[489] Source : vox.com (https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram).

### **3)** Hacking *versus* information : parangon du couple agilité/paralysie ?

Pour tester notre appareillage théorique, il convient d'en articuler les différents étages. De fait, il paraît pertinent d'imbriquer les trois grilles de lecture pour en tirer une matrice dans laquelle vient opportunément s'insérer l'architecture du cyberespace. Partant de l'approche communément admise d'une partition de ce dernier en trois couches, le schéma ci-dessous précise notre réflexion.

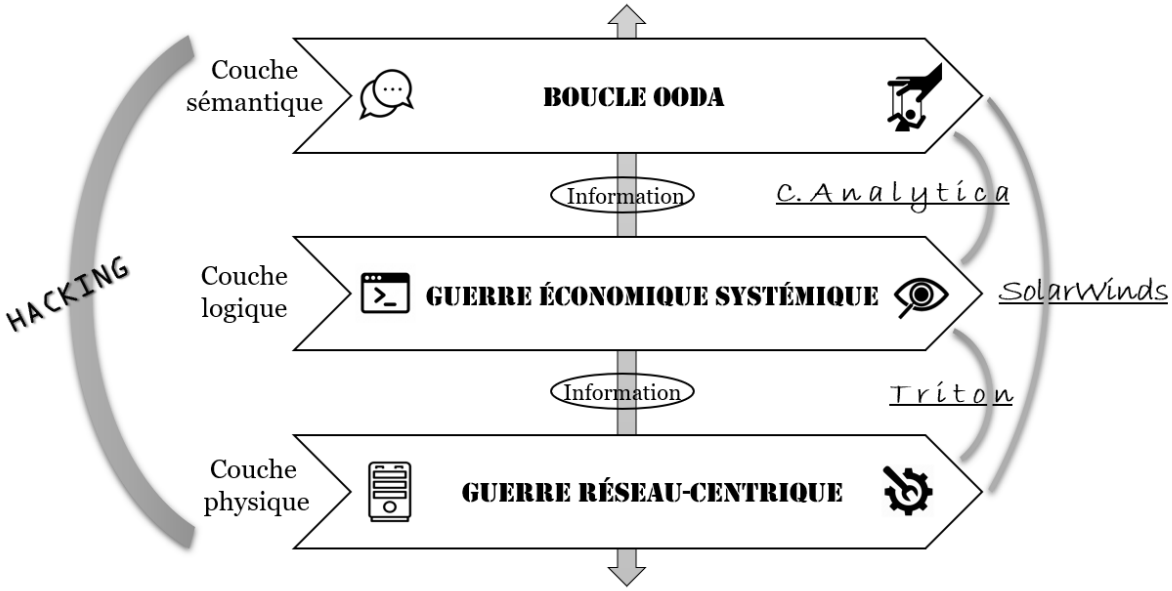



**Figure 36 :** *Le hacking comme fer de lance de l'infoguerre*

Source : Yannick Pech, 2021.

#### **a)** ***Hacker la couche physique : Triton et la guerre pour, par et contre l'information***

D'après l'étude approfondie de Carcano/Dragoni/Krotofil (2018), cette attaque a comporté trois phases : initialement, une collecte d'information technique sur le SCADA|SIS (plateforme *Triconex* de Schneider Electric) (pour) ; ensuite, l'achat de tout ou partie du système pour rétro-ingénierie logicielle (par) ; enfin, la communication avec le SIS pour lui envoyer de fausses informations et ainsi le contrôler (contre).

### *L'architecture réseau-centrée autorise l'attaque cyber-physique de Triton*

La *Network Centric Warfare* met en lumière les opportunités de « l'effet réseau » décrit par la loi de Metcalfe[490]. Si le maillage des hommes et des machines en augmente la valeur, cette hyperconnectivité en accroit également la surface d'attaque. L'analogie permet de comprendre que les capteurs, contrôleurs et actuateurs du SCADA ciblé sont à l'image du triptyque capteurs-décideurs-acteurs du modèle infocentré. L'agent décideur (le Triconex) est ici piraté pour générer le dysfonctionnement d'un système de *sécurité* qui devient par là même objet de *sûreté*, dès lors que l'attaquant vise à provoquer intentionnellement un accident.

On peut donc parler, d'une part, d'un *effet de levier réticulaire*[491] d'ordre socio-informationnel : en effet, l'analyse de Triton démontre à quel point il est désormais aisé de faire du renseignement sur la base d'informations blanches : moteurs de recherche, forums (GitHub, Scribd), bibliothèques de programmation (FQFA[492]), marchés en ligne (Alibaba, Ebay), LinkedIn (personnes-clés, profils haut niveau), outils dédiés (*Shodan*[493], *VirusTotal*, pièces de codes malveillants et kits d'*exploits* sur étagère)… Autant de ressources qui permettent d'abaisser mécaniquement le niveau de sécurité des SCADA – on peut acheter en ligne le manuel et même des modules du Triconex (entre 2K et 10K$). D'autre part, on constate un effet de levier réticulaire d'ordre technique, avec articulation des couches matérielle et logicielle pour agir sur le monde physique. Triton pose un jalon inédit car il vient flouter la limite entre guerre cinétique et guerre cybernétique. C'est d'ailleurs dans un contexte plus large de nature géoéconomique que vient se placer Triton.

### *Le test hors limite de Triton : au-delà de la guerre économique ?*

Les États s'associent à des organisations de hackers pour servir leurs buts de guerre. Triton est assurément le fait d'une APT-corsaire. Si le Kremlin est incriminé, il est toutefois plausible d'imputer l'attaque à l'Iran dont on connaît l'inimitié profonde et mutuelle avec le régime des Saoud, et le passif des offensives portées contre la monarchie. Le cyberespace est un instrument ambivalent à la charnière de la force et de la ruse. En l'occurrence, ciblant une entreprise nationale énergétique, Triton est une arme politico-économique de cybercoercition. L'encerclement cognitif se traduit ici par la dissimulation des mouvements à l'œuvre dans le cyberespace, marqueur et vecteur insaisissable de la puissance-influence. Dans ce contexte concurrentiel, il importe de décider vite mais surtout bien.

[490] La loi de Metcalfe, qui porte le nom de son inventeur, Robert Metcalfe, détermine que la valeur d'un réseau de communication est égale au nombre de terminaux connectés au carré. C'est « l'effet de réseau » lié aux TIC.
[491] Christian Marcon & Nicolas Moinet, *Stratégie réseaux*, *op. cit*.
[492] *First Qualified/First Admitted* (FQFA). Processus de validation de bibliothèques logicielles.
[493] Shodan est parfois qualifié de « Google des hackers » (https://www.shodan.io/). Il s'agit d'un site web inventoriant les objets connectés vulnérables accessibles depuis l'Internet.

***Triton à l'aune de la boucle OODA : un dispositif saoudien perturbé***

Le royaume était en capacité d'anticiper ce type d'attaques alors que notamment les SCADA de la société Aramco avaient plusieurs fois fait l'objet de tentatives d'intrusion. De plus, l'année 2017 est émaillée de nombreuses offensives concentrées (*Shamoon 2*, campagnes de phishing). Triton révèle une montée aux extrêmes face à laquelle les Saoudiens sont restés aveugles (*cry-wolf syndrome*[494]). C'est ce que vient appuyer le rapport du *think tank* américain GFCSR, concluant en 2019 à la mauvaise formation des acteurs locaux et la méconnaissance des enjeux nationaux de cybersécurité[495]. Ce à quoi répond aujourd'hui Ryad en fondant sa politique de développement *Vision 2030* sur un pilier de cyberdéfense et la promotion d'une « cyber-conscience ».

En définitive, des opérations itératives diversifiées sur le temps long ont brouillé l'image mentale construite par le royaume à propos du risque cyber. À l'image de son long aveuglement sur la nécessité impérieuse de diversifier une économie de rente, Ryad a minimisé les capacités cyberoffensives de ses rivaux. Le royaume a compris tardivement que toutes ces attaques, quoique manquées, visaient à expérimenter et affiner un savoir-faire en constante progression et des méthodologies toujours plus pointues. Dès lors, l'Arabie saoudite a vu sa boucle OODA rallongée, et son action (A) entravée par un processus décisionnel embrouillé (D) du fait d'une perte de repères (O) conduisant à sa cécité (O). Son « cyber-besogneux » adversaire, lui, raccourcit sa boucle en favorisant, d'une part, un esprit d'initiative (A) fondé sur une décision éclairée (D), grâce à la construction d'un schéma cognitif lucide (O) sur l'effet de levier induit par le cyberespace ; d'autre part une observation claire de l'état des forces de Ryad sur la cybersécurité (O). Appuyé depuis 2012 par des équipes états-uniennes, le pays semble en effet accuser le coup de son impréparation à la cyberguerre. Triton s'apparente à une opération commando, à classer parmi les émergents « hacks de classe olympique » (*Hacking Olympics*), sorte d'attaques-tests sur environnement physique temps-réel. En somme, son inertie a paralysé Ryad. Cela arrive aux « meilleurs », comme le montre l'affaire SolarWinds.

### b) *Hacker la couche logique : SolarWinds et la guerre pour, par et contre l'information*

La particularité du cas SolarWinds est sa nature d'attaque dite « de chaine logistique ». C'est *in fine* par la compromission d'un simple logiciel que ce type d'attaque peut se déployer et toucher sous-traitants comme fournisseurs ou clients. En effet, les États et entreprises sont aujourd'hui dépendants de solutions logicielles commercialisées par un oligopole de sociétés

[494] Syndrome de banalisation des alertes (trop fréquentes) émises par les services de renseignement, se révélant être des faux-positifs.
[495] gfcyber.org/cybersecurity-challenges-of-the-ksa-past-present-and-future/

du numérique. Cette imbrication entre organismes publics et prestataires privés engendre une interdépendance qui rend toujours plus vulnérable une organisation désormais holistique.

### *Orion : chainon faible ou verrou d'une galaxie réticulaire ?*

Classés plus grande cyber-puissance et sans réel équivalent[496], les États-Unis ont pourtant subi de nombreux assauts en matière d'attaques par rebond. Comme il est coutume de dire, la sécurité d'un système s'évalue à l'aune de son maillon faible. Or, indépendamment de sa supposée faiblesse, l'infrastructure logicielle d'Orion a été ciblée pour sa position cruciale, à l'intersection d'une galaxie d'acteurs économiques et politiques de premier plan. Cette réticularité rend le cyberespace trop hétérogène dans ses parties prenantes. La fusion des SI entre les points nodaux que constituent les entreprises et leur écosystème tactique entrave une harmonisation des critères d'exigences de la sécurité. Si on ignore comment les hackers ont opéré, la procédure d'accès rudimentaire aux serveurs d'Orion via un mot de passe faible (« solarwinds123 ») de surcroît mentionné publiquement sur GitHub, a été notifiée à SolarWinds dès 2019 par un expert en informatique[497].

### *Hacking et guerre systémique : porter le glaive partout où stratégie fait loi*

D'après Christian Harbulot[498], la guerre économique est systémique parce qu'elle oblige les États à dissimuler leurs attaques informationnelles par l'orchestration indirecte de jeux d'acteurs présents sur plusieurs échiquiers. Dans le cas de SolarWinds, le hacking est le fer de lance d'une guérilla informationnelle visant à subvertir la prédominance américaine. Si un encerclement cognitif global américain est à l'œuvre par le biais de normes et d'une extraterritorialité judiciaire, il l'est également au travers du cyberespace dont la stratégie nationale de 2018 témoigne de la volonté des États-Unis de façonner une infrastructure et un marché de la cybersécurité conformes à leurs intérêts. Ainsi, Russie et Chine n'auront de cesse d'accroitre leurs capacités de déstabilisation en jouant sur tous les échiquiers dont le cyber est le plus permissif et un démultiplicateur de force. Car, au-delà d'une campagne d'espionnage de grande envergure, le cas SolarWinds est une atteinte à la réputation de la cyberpuissance. « L'espace informationnel » de la doctrine Gerasimov permet en effet l'utilisation de techniques asymétriques pour saper les capacités de l'adversaire. Les États-Unis y répondent par des représailles économiques, et brandissent la menace du *hack back*. Mais n'est-ce pas jouer le jeu d'un Kremlin qui ne s'embarrasse pas de questions éthiques à l'égard de la

[496] iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
[497] cyberguerre.numerama.com/10676-les-dirigeants-de-solarwinds-accusent-un-stagiaire-de-la-fuite-du-mot-de-passe-solarwinds123.html
[498] Christian Harbulot, « Chine/Etats-Unis ? Sortie de crise ?..., *op. cit.*

*cyberguerre* ? Dans cet affrontement cognitif, c'est l'attaquant qui a toutes les chances de l'emporter.

### ***Surprise opérative & agilité tactique* VS *inertie mentale & excès de confiance***

Déployée un an avant sa découverte, la campagne instiguée contre SolarWinds a été accompagnée d'autres vecteurs d'attaques (phishing) en amont et aval pour tenter de prolonger l'offensive initiale. L'attaquant part donc avec une longueur d'avance d'autant qu'il agit furtivement et trompe ses victimes par des techniques d'ingénierie sociale. Le combat n'a même pas eu lieu, car les États-Unis ont observé le champ de bataille avec les mauvaises lunettes tactiques. Dans le contexte post-électif de 2016, on ne s'attend pas à essuyer une attaque depuis la chaine de production d'un fournisseur de logiciels en outre assez commun(s). Sur le plan opératif, les auteurs ont commis leurs forfaits « *depuis l'intérieur des États-Unis* » concède la Maison-Blanche[499], sans pour autant apporter de réponses sur les manquements du renseignement et de la cyberdéfense. En somme, l'attaquant a leurré sa victime par l'usage d'offensives tactiques novatrices en touchant là où on ne l'attendait pas, générant un mécanisme de dissonance cognitive. La prime en revient à l'attaquant dans un milieu stratégique où la guerre irrégulière est la norme et la législation, l'exception.

Techniquement parlant, si on plaque le mode opératoire du hacking au schéma de Boyd, on comprend mieux l'ascendant des assaillants sur leur antagoniste. Dans la méthodologie de l'attaquant que décrit par le menu le hacker « Maître » Oda (2021)[500], l'information fait en première intention l'objet d'une *reconnaissance passive* (OSINT) et/ou *active* (ingénierie sociale, *scanning*), du maintien à son accès et, en dernier ressort, d'une offuscation visant à dissimuler les opérations précédentes, *i.e.* ses propres informations (identités physique & logique, empreinte numérique et signature opératoire). Dans notre cas, les activités de reconnaissances passive et active initiées très tôt permettent aux attaquants une observation clinique – à l'intérieur des lignes – des défenses adverses (O) ; le contexte politique favorable évoqué plus haut leur assure une *conscience situationnelle* objective sur les failles américaines (O) ; on peut assimiler le gain/maintien d'accès et l'élévation de privilèges[501] à la pénétration de la boucle adverse, l'offuscation assurant la furtivité de l'attaque à l'insu de la cible ; le processus de décision (D) est planifié sur le long terme (APT) et les actions fluides (A). À

[499] cyberguerre.numerama.com/10516-laffaire-solarwinds-bien-plus-quun-simple-incident-despionnage-pour-la-maison-blanche.html

[500] Alexandre « Maître » Oda, est entrepreneur et hacker éthique. Voir https://web.archive.org/web/20220817083321/https://oda-alexandre.com/cybersecurite, site web indisponible depuis fin 2022. On parle beaucoup d'OSINT, dans le milieu SSI globalement, à propos des phases de reconnaissance dans les cyberattaques, selon Jean-François Loewenthal (entretien du 26/06/2017).

[501] Prendre le contrôle administrateur sur un système d'information.

l'inverse, côté victime, un simple email de phishing jouera sur les actes-réflexes d'un utilisateur dont l'image mentale n'impliquera aucune vigilance particulière, notamment en environnement organisationnel quotidien. La duperie reste le principal levier pour miner les défenses adverses, impliquant une perte ou absence de repères dans la phase d'orientation et entrainant, par cascade, la friction sur les trois autres processus. Le discours sur « l'erreur du stagiaire » clamé dans un premier temps par la direction de SolarWinds est représentatif de la confusion d'un dispositif perturbé. Le cas SolarWinds illustre les failles de la cyberpuissance occidentale. Quant à l'affaire Cambridge Analytica, elle est le signe paradoxal d'un effet boomerang de la suprématie technologique états-unienne.

### c) *Hacker la couche sociocognitive : Cambridge Analytica et la guerre pour, par et contre l'information*

Parmi les cas les plus documentés de ces dernières années, l'écheveau Cambridge Analytica/Facebook s'avère toutefois complexe à démêler. Et pour cause, nous nous situons ici au dernier niveau de la guerre informationnelle, l'affrontement cognitif. Celui-ci se déroule sur la couche éponyme du cyberespace, où l'aspect psychologique prend une dimension virale. Cette affaire est éloquente sur les pratiques de manipulation de l'information à des fins lucratives ou politiques. Les hautes technologies semblent désormais enfermer l'humanité tout entière dans un auto-encerclement cognitif où se jouent des luttes d'influence perpétuelles.

#### *Dynamique réseau-centrique de la viralité déceptive*

Inspirateur de la NCW militaire, le monde politico-économique américain a su utiliser cet effet de levier en propulsant les sociétés de la Silicon Valley au sommet de la chaine de la prédation. Vantant les mérites humanistes des « autoroutes de l'information » et le rêve d'un *village mondial*, elle se sont insidieusement approprié nos esprits en diffusant des standards adoptés panurgiquement. Là est l'un des piliers de l'encerclement cognitif opéré à l'endroit des alliés des États-Unis. L'on comprend dès lors que Chine et Russie y opposent un principe de souveraineté numérique, proposant des contre-modèles ou jouant dans la même cour concurrentielle. Cet encerclement passe aussi par l'information. La double acception du mot *déceptif* permet de caractériser les opérations psychologiques (*PsyOps*) menées sur les RSN : générer à la fois désillusion et tromperie, gagner par la positive ou ne pas perdre par la négative.

#### *Persuader, convaincre, soumettre par la technologie*

Les États-Unis eux-mêmes sont victimes de leur sujétion à la technologie. L'essor des attaques informationnelles et informatiques démontre combien les rapports du fort au faible

sont dynamités par l'effet de levier des réseaux. Si le *Grand Hack*[502] est le fait d'acteurs économiques anglosaxons, la Russie a pu démultiplier son avantage grâce à la boîte de Pandore ouverte par les prescripteurs et bénéficiaires du *dataïsme*. La mise en abîme réticulaire des mécanismes décrits par Christopher Wylie donne le vertige (figure n°35). Ce dernier parle de tactiques fallacieuses pour parvenir *primo*, à collecter indirectement des données par la permissivité de l'ingénierie logicielle de Facebook et, *secundo* les exploiter en vue d'influencer un ensemble d'utilisateurs à même de contrebalancer la volatilité électorale.

Tous les critères définis par le concept d'encerclement cognitif[503] sont réunis, et ce sur le seul échiquier numérique :

- Pas d'ancrage national (mais transnational) du protagoniste-clé (Cambridge Analytica) ;
- Dissimulation derrière un Facebook complaisant[504] ;
- Légitimité d'une pratique déjà employée par d'autres équipes (Obama…) sous couvert de marketing politique, et image positive du *big data* ;
- Exploitation et légitimité de la technologie de RSN ultra-démocratisée en Occident ;
- Ciblage de profils actionnables (« idiots utiles ») via *trolls* et *bots*[505].

Le rôle de Facebook semble majeur car il met en connexion (via *Facebook Login*, une technologie d'authentification unique) le créateur d'une application anodine avec une officine privée de collecte et d'analyse dont les moyens auraient fait rêver la Stasi. Comme l'indique Alexandre Oda[506], Facebook est « *un outil de propagation et un vecteur d'influence.* » Appelé à répondre de sa responsabilité, le PDG de Facebook minimise la portée de l'affaire et fait comme de coutume acte de contrition. Mais au-delà d'une énième négligence en termes de sécurité des données, comment seulement remettre en cause la conception d'une technologie pensée pour la mise en réseau et la surveillance, même indirecte ? Facebook, au corps défendant des Américains, ne devient-il pas, comme l'ont déjà montré les révélations d'Edward Snowden (programme *PRISM*), un véritable cheval de Troie ?

### *L'art de la supercherie à l'ère numérique*

Si l'on tient compte de sa responsabilité (condamnation et liquidation judiciaires), il convient de considérer Cambridge Analytica comme l'attaquant. Comment, dès lors, la firme

[502] *The Great Hack*, titre d'un documentaire sur l'affaire Cambridge Analytica/Facebook produit par Netflix.
[503] Christian Harbulot, « Chine/Etats-Unis ? Sortie de crise ?..., *op. cit.*
[504] lemonde.fr/pixels/article/2019/02/18/les-deputes-britanniques-etrillent-facebook-pour-son-role-dans-les-campagnes-de-desinformation_5424886_4408996.html
[505] Emerson T. Brooking & Peter W. Singer, *LikeWar: The Weaponization of Social Media*, HMH Books, 2018, 416 p.
[506] Entretiens avec l'auteur, 09/07/2020 et 16/06/2021.

s'y est-elle prise pour influencer les usagers-citoyens dans leur décision de vote ? En occupant le territoire informationnel où se joue la bataille cognitive. Délibérément ou inconsciemment, l'application créée par l'enseignant-chercheur en psychologie est le premier cheval de Troie dont la plateforme Facebook constituera le second *proxy* et Cambridge Analytica le bénéficiaire final des données que le premier lui livrera contractuellement. Dès 2014, un collègue psychométricien d'Aleksandr Kogan signale auprès des autorités de l'université que les activités de ce dernier peuvent porter préjudice à l'établissement. Cachées dans la lumière, les dispositions de la politique de confidentialité de Cambridge Analytica sont éloquentes : la firme précise collecter des données personnelles par le biais d'applications tierces. Quant à Facebook, la société masque son opacité dans la gestion des données d'utilisateurs derrière un vernis de transparence suffisant à les rassurer.

Tous les scandales liés à des fuites de données le confirment, l'addiction technologique aveugle les usagers des TIC sur le détournement de leurs informations personnelles. Les propos d'Alexandr Kogan vont dans ce sens : « *Je pense que l'idée que nous avions, à savoir que tout le monde est au courant et s'en fiche, était fausse*.[507] » Cet état de fait est le produit d'un schéma cognitif total, où les vertus des TIC masquent leur face noire. La firme britannique a habilement orchestré et mobilisé un jeu d'acteurs en vue de remplir sa mission. Elle s'est ainsi appuyée sur la partie intermédiaire (les usagers de Facebook) en :

- exploitant son aveuglement et des biais cognitifs décuplés par le numérique et arsenalisés par des IA (*Ripon*) et des trolls (Observation) ;
- perturbant son appréhension des risques de confidentialité inhérents aux CGU et API[508] de Facebook, sans parler de la désinformation endémique du RSN (Orientation) ;
- facilitant la diffusion des fuites du parti démocrate (la partie adverse) issues du hack de John Podesta – exploité par WikiLeaks –, combinant à dessein le produit de l'ingérence russe et le propre fruit de ses manœuvres manipulatoires (Décision–Action).

Au bilan, plus que l'efficacité – sujette à caution – des actions de Cambridge Analytica, ce sont les stratagèmes employés qui augurent de l'épanouissement d'une ère dystopique de *post-vérité* dont on prend peu à peu la mesure.

[507] wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica/
[508] CGU : conditions générales d'utilisation ; API : interface de programmation applicative (IPA).

### Enseignements

Le hacking, comme technique au service de la maîtrise de l'information constitue un objet de recherche pertinent pour l'IE. La primo-analyse de ce corpus donne déjà quelques éléments de réflexion. En premier lieu et schématiquement, chaque grille de lecture éclaire les pratiques du hacking dans la guerre de l'information. Celle-ci ne peut se penser en dehors du cadre matriciel qu'est le cyberespace :

- **La *Network Centric Warfare* pose l'ossature par laquelle l'information, dans sa dimension technique, circule (couche physique). L'infoguerre utilise l'effet de levier réticulaire technique de ce support.**
- **La guerre économique systémique pose la *matrice logicielle* des rapports de puissance (couche logique). L'infoguerre utilise l'effet de levier réticulaire socio-informationnel de cette « image vectorielle ».**
- **La boucle OODA pose la stratégie que déploient les acteurs pour encercler cognitivement leurs adversaires (couche sociocognitive). L'infoguerre consiste à paralyser l'autre camp et mobiliser le sien.**

En second lieu, notre analyse a révélé que le hacking est une composante essentielle sinon cruciale de la guerre de l'information dès lors qu'il s'agit d'obtenir avant l'adversaire une connaissance actionnable pour saboter et dissimuler ou subvertir et manipuler. Il joue ainsi un rôle éminent dans cette guerre qui se joue à trois niveaux :

- L'appropriation (pour l'information) ;
- L'interdiction (contre l'information) ;
- La manipulation (par l'information).

Si les conclusions de l'analyse des cas présentés autorisent une généralisation, on peut dès lors estimer comme déterminant le rôle tenu par le hacking dans cette guerre.

**L'analyse de l'attaque Triton (appropriation pour interdiction/manipulation, *in fine* destruction) a révélé l'importance de l'effet de levier dans une logique de réseaux où mondes physique et numérique fusionnent progressivement**. La grille de lecture de la guerre réseau-centrique apporte ainsi un éclairage utile sur l'impact des opérations de hacking visant à détruire des objets matériels par l'intermédiaire d'attaques logicielles. Pensons aux attaques cyber-électro(méca)niques sur les objets connectés qui n'en sont qu'à leurs balbutiements. Visant une entreprise étatique dans le domaine de l'énergie, Triton s'inscrit dans une logique de rapports de puissance géoéconomiques que le cadre conceptuel de la guerre systémique permet d'appréhender. Enfin, l'inertie de l'État saoudien

s'explique par un manque de vision stratégique et une image mentale erronée qu'illustre l'application de la matrice OODA.

**Le cas SolarWinds (manipulation-altération pour appropriation et subversion) a montré, pour sa part, qu'un monopole sur les infrastructures matérielles et logicielles du cyberespace pouvait avoir un effet contreproductif**. En l'occurrence, le maillage techn(olog)ique et commercial états-unien offre une surface d'attaque accrue dans un contexte de guerre systémique où la fin justifie les moyens (espionnage, sapage de la réputation et de la puissance), comme le montre cette attaque attribuée à la Russie. La boucle OODA a permis d'en décrypter les subtils mécanismes tout en illustrant la paralysie stratégique américaine.

**L'affaire Cambridge Analytica (appropriation via exploitation logicielle et psychologique pour manipulation) a, de la même façon, permis de mettre en exergue les vulnérabilités induites par l'effet de levier réticulaire technique (les « tuyaux ») et technologique (les contenus) des réseaux socionumériques**. Les manipulations ou compromissions informationnelles brouillent les jeux d'acteurs – y compris démocratiques – susceptibles d'entrer dans le cercle vicieux de la tyrannie de la communication.

**En définitive, sur fond de guerre économique dont les soubassements techniques et les étages cognitifs sont centrés sur les réseaux *lato sensu*, le cyberespace se présente comme l'échappatoire suprême pour dissimuler ses manœuvres stratégiques et contourner les règles de bienséance d'une hyper-compétition générale en réalité biaisée**. L'anthropologue Bernard Traimond nous le dit : « *L'économie n'existe pas, c'est de la politique !* »[509] Tout comme l'est l'économie dans les rapports de puissance, le hacking est l'arme d'une guerre à visée déportée. Une arme qui égalise les rapports de force par la profonde remise en question du couple traditionnel fort/faible. Il apparaît dès lors comme l'instrument privilégié de ce piratage des normes tant du point de vue de la sécurité collective que de la suprématie économique internationales. **Le hacking, c'est *l'opération spéciale permanente*, dans tous les sens du terme : comme outil militaire efficient, fulgurant et parfois décisif ; comme opération de promotion, littéralement de propagande quand il s'agit de manipuler les masses**.

Un état de cybersécurité est-il du moins possible ? La guerre réseau-centrique permet d'appréhender la nature éminemment réticulaire et holo-connectée des rapports de conflictualité. L'enjeu repose ici sur la recherche de la maîtrise technique et technologique où

[509] Bernard Traimond, *L'économie n'existe pas*, Le Bord de l'Eau, 2011, 114 p.

vient s'arrimer le débat sur l'autonomie stratégique et la souveraineté numérique, avec les difficultés que l'on connaît en France. Ce débat, avec par exemple l'épineuse question de l'hébergement des données nationales de santé, nécessite de mesurer notre dépendance et penser notre indépendance vis-à-vis d'acteurs étrangers comme les États-Unis. Cela vaut sur le plan militaire comme civil. Sans quoi notre cybersécurité n'est même pas entre nos mains.

Dans ce sous-chapitre nous avons traité de cas de hacking illégal et/ou « immoral ». Mais la catégorie – si elle existe véritablement – des *hackers éthiques* doit assurément être prise en compte dès lors que l'on parle de cybersécurité. Ainsi, par leur expertise à la fois technique et psycho-sociologique, les hackers connaissent bien les arcanes des réseaux physiques et humains. Présentés parfois comme le système immunitaire de l'organisme numérique, leurs compétences sont paradoxalement sous-exploitées. Et bien que leur image commence à se normaliser et qu'ils soient davantage sollicités par l'État ou les entreprises depuis quelques années, il semble utile de sonder les relations véritables que ces acteurs entretiennent ensemble.

# III. L’intelligence cyber comme boussole stratégique

# Chapitre 5 | Quatre cas au prisme d'une intelligence économique du cyber

Dans le chapitre 4, nous avons pu appréhender la guerre appliquée au cyber dans une acception large, entre conflictualité informationnelle et attaques informatiques. À travers la supra-analyse de cas consacrés à cette cyberguerre, nous avons montré que le hacking pouvait être présenté comme la pointe avancée des guerres de l'information puisqu'il exploite les trois couches du cyberespace en vue de hacker des réseaux, des systèmes logiciels ou encore des esprits. Désormais, il nous faut analyser les liens qu'entretiennent les hackers avec les institutions afin d'apprécier leur nature dans la perspective d'une stratégie intégrale de cybersécurité nationale.

## A. *Corpus documentaire et cheminement analytique*

Nous présentons ici les cas soumis à la grille théorique complétés de témoignages de profils de différents horizons. Par ailleurs, sera explicitée la démarche analytique appliquant l'appareillage théorique que nous avons défini à partir de l'intelligence économique.

### 1) Le corpus : cas et entretiens

Le corpus utilisé pour notre étude est constitué de quatre cas et d'une série de 35 entretiens réalisés entre 2017 et 2023.

S'agissant des cas sélectionnés, nous devons en premier lieu souligner les difficultés éprouvées à l'identification d'évènements ou au mieux de situations significatives qui puissent faire l'objet d'une étude selon les canons établis par les sciences sociales. Étant entendu par ailleurs que la grille théorique élaborée à partir de l'intelligence économique est le fruit d'une approche réflexive à la scientificité relative. Tout comme l'est du reste objectivement considérée la démarche abductive qui a servi de fil conducteur à notre travail. Aussi, ces analyses présentent un caractère éminemment exploratoire et interprétativiste.

**Les quatre cas considérés sont les suivants :**

- *Cas n°1* : l'affaire « Bluetouff » met en scène les rapports d'incommunication entre les autorités judiciaires et le *journaliste-hacker* Olivier « Bluetouff » Laurelli, au cours d'un procès ayant au moins permis d'éclairer la notion de « vol numérique ». Ce cas, qui date

des années 2012-2015, reste très actuel et a été choisi parce qu'il reflète le manque de culture numérique des institutions judiciaires et le déphasage entre l'état d'esprit d'un hacker et « l'esprit des lois ». En outre, nous avons pu nous entretenir avec Olivier Laurelli.

- *Cas n°2* : nous avons voulu réaliser une étude longitudinale sur la place et l'image de la figure du hacker au sein des institutions publiques et en particulier auprès des législateurs. Le point de départ en a été la publication de la *Stratégie nationale pour la sécurité du numérique* de 2015 suivie de l'entrée en vigueur de la *Loi de 2016 pour une République numérique*, pour s'achever avec la mission d'information sur la souveraineté numérique nationale et européenne de 2021. Ce choix a été fait en vue de sonder la manière dont les acteurs politiques appréhendent les hackers en particulier et les TIC en général. L'analyse des corpus documentaires législatifs témoigne globalement d'une incompréhension encore manifeste du statut et du rôle des hackers éthiques dans notre pays.

- *Cas n°3* : sont ici considérées les vagues de cyberattaques qui ont touché des hôpitaux entre 2020 et 2022 en particulier. Ces atteintes déstabilisent grandement les établissements médicaux : il leur faut en moyenne entre 12 et 18 mois pour se remettre de ces crises. Tout l'intérêt de ce suivi de situation synthétisé en un cas réside, d'une part, dans son actualité – en regard du degré de maturité cyber en théorie accru –, d'autre part dans les retours d'expérience que certains établissements ont utilement publié à des fins de sensibilisation.

- *Cas n°4* : ce dernier porte sur le parcours hors norme, significatif et édifiant d'un hacker français, dont le parcours chaotique peut expliquer une certaine frilosité institutionnelle, mais qui est révélateur de la difficulté à intégrer ce type de profil dans des stratégies de cybersécurité. Ce cas a été tout naturellement sélectionné pour son caractère rare et s'appuie à la fois sur les Mémoires de Florent « Theeeel » Curtet, publiés à l'été 2023, et sur les entretiens que nous ont accordés Florent Curtet lui-même et l'officier de police qui l'a appréhendé puis soutenu et enfin recommandé.

### Les entretiens :

Leur nombre se porte à 35. Ils sont convoqués aussi bien dans le cadre de ces études de cas que dans l'ensemble du travail de thèse. Ils ont été réalisés entre 2017 et 2023 auprès de différentes catégories de profils placées au carrefour du monde cyber (émanations de l'État, du monde de l'entreprise et de l'expertise du numérique)[510] :

[510] Voir le verbatim des entretiens en annexes. Leurs statut, fonctions et expertises y sont mentionnés.

- chercheurs en institut privé et universitaires (spécialistes) ;
- gendarmes et policiers (N-TECH, renseignement/IE) ;
- entrepreneurs/managers/chefs d'entreprises (en rapport avec le domaine) ;
- consultants et spécialistes en IE ;
- anciens ou actuels cadres du renseignement d'État (DRSD, DGSI) ;
- experts en cybersécurité (RSSI, ANSSI, dont un chercheur-hackeur sous pseudonyme mais anonymisé. Nous l'appellerons « Bob ») ;
- hackers (huit « éthiques/blancs », un hacktiviste/gris et une « hacktiviste/grise » anonymisée. Nous l'appellerons « Alice »).

Ces deux derniers types ont été distingués en vertu des statuts professionnels, état d'esprit et vision du sujet propres à chaque individu, ainsi qu'à leur choix d'auto-qualification (spécialiste cybersécurité *ou* hacker).

Enfin, deux profils (ex-DGSE/Armée) ont été contactés mais n'ont pas souhaité répondre (sur ce sujet spécifique) tout en communiquant implicitement certains détails. Ils seront mentionnés nommément.

Au début, les entrevues ont été pilotées par un guide d'entretiens[511], et leur forme était semi-ouverte. Leur durée a été de 1h à 1h30 chacun. Nous avons fait le choix d'abandonner le guide au fil des rencontres car il ne nous a pas paru pertinent ni pragmatique ; ce qui a conditionné le passage à des entretiens ouverts fondés sur une question très large comme point de départ (nature des rapports hackers-autorités publiques/organisations privées, état de la cybersécurité en France). Cela s'est avéré plus fructueux car les protagonistes se sentaient dans un cadre plus informel et un climat serein, et estimaient la parole libre et l'objectif limpide en dépit de la difficulté et de l'envergure du sujet. Plusieurs thématiques connexes ont pu être évoquées et approfondies, qui ont un rapport étroit avec les enjeux et les questions posés par l'intelligence économique. Sans exhaustivité : souveraineté numérique ou plus générale, appréciation des politiques gouvernementales, culture stratégique des élites, etc.

Lorsque l'expression « forces de sécurité » est employée, elle désigne l'ensemble des entités étatiques en charge de la sécurité et de l'ordre public, de la protection de la nation et du renseignement : unités de police, gendarmerie, services spéciaux, agences telles que l'ANSSI ou états-majors tels que le COMCYBER spécialisés dans la sécurité du numérique.

[511] Voir annexes, entretiens.

## 2) Appareillage théorique et cheminement analytique

### Grille théorique :

La mise en application de notre grille de lecture nécessitera d'assouplir l'appareillage des caractéristiques (« théoriques », « pratiques », « clés ») du modèle. Les voici pour rappel sous forme de schéma :

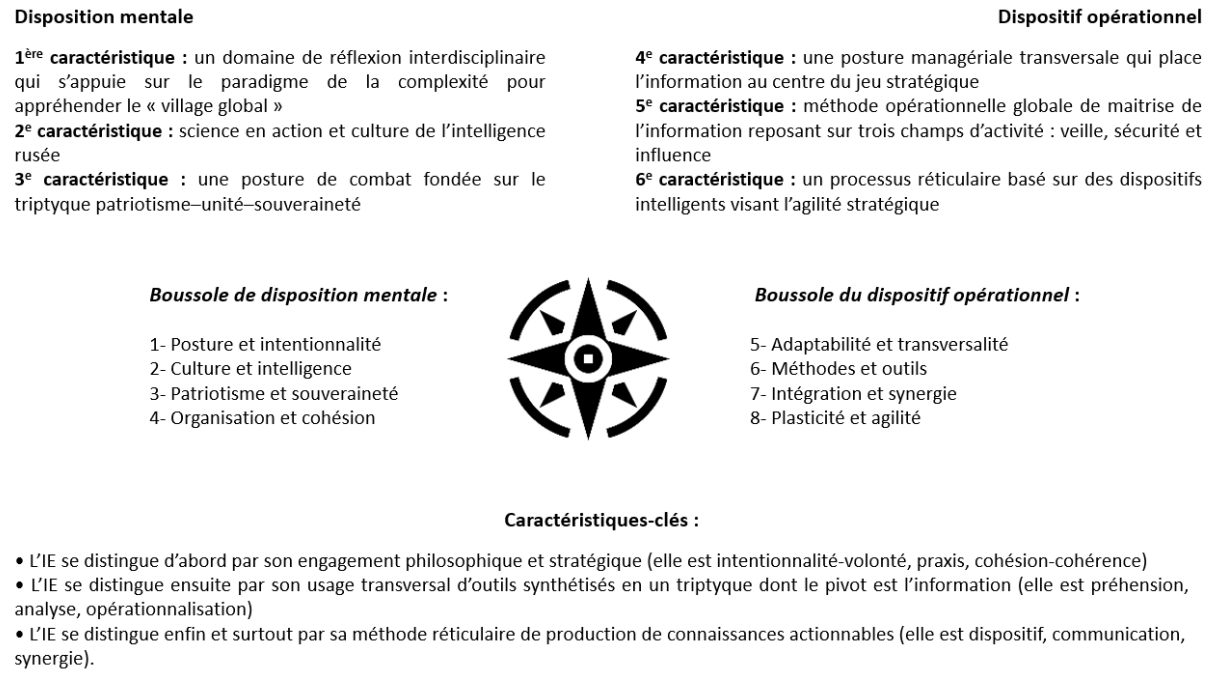



**Figure 37 :** *Grille théorique synthétisée sous forme de schéma*

### Cheminement analytique :

- Les caractéristiques relevant de la *disposition mentale* seront abordées selon une observation déportée puisque relevant d'un champ symbolique.
- Les caractéristiques de *dispositif opérationnel* seront appréhendées globalement par observation empirique, mais enrichies des témoignages issus des entretiens.
- Les « *boussoles* » nous serviront à évaluer le « cap » suivi par les acteurs des situations étudiées.
- Les *caractéristiques-clés* permettront de dégager une synthèse du cheminement réflexif en répondant au mieux aux hypothèses issues de notre problématique.

## **B.** *Sonder les liens qu'établissent hackers et institutions*

Précisons notre démarche en partant des propos de la hackeuse israélienne Keren « k3r3n3 » Elazari :

> « *Il y a une relation d'amour-haine entre l'État et les hackers. Parce que ceux qui les diabolisent sont les mêmes qui les utilisent largement. Les hackers sont les seuls capables de contrebalancer et de jouer dans la même cour que les États invasifs et les entreprises dévoreuses de données. On voit les hackers comme des héros, alors pourquoi dans le même temps continuer à les considérer comme les méchants ?* [512] »

Dans ce sens, nous posons comme hypothèse forte que les hackers forment le chainon manquant de la cybersécurité de pays tels que la France. Pour cette raison, il semble opportun d'étudier les rapports qu'ils entretiennent avec les autorités publiques ou des organisations privées. Ce faisant, et parce qu'ils connaissent finement les rouages du cyberespace, de la nature de ces relations peuvent dépendre le développement voire les fondements de la cybersécurité nationale. Ces liens sont-ils solides, s'inscrivent-ils dans la matrice stratégique de l'IE où l'esprit « réseau », la communication et l'intelligence collective sont essentiels ? Ou sont-ils fragiles, distendus, basés sur des intentions biaisées ?

Nous reprenons les trois hypothèses qui ont émergé de notre approche abductive :

> 1 – ces trois mondes (hackers–État–entreprises) sont intégrés et dans une co-construction (interaction et communication décloisonnées, projets communs, logique de dispositifs intelligents, synergie…).
>
> 2 – ces trois mondes sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas (incommunication) par manque de synergie.
>
> 3 – ces trois mondes s'ignorent (acommunication – Wolton, 2019).

Nous les soumettrons à l'examen des cas pour en tirer des enseignements à même de répondre à notre problématique de recherche.

[512] Keren Elazari, Conférence TED, 10/06/2014. Traduction par nos soins.

### 1) L'affaire « Bluetouff » : reflet d'une Justice encore peu adaptée aux questions cyber

« *Par défaut, les hackers sont perçus comme une menace par les autorités*.[513] »

Olivier Laurelli

L'affaire Olivier Laurelli, de son pseudonyme « Bluetouff », donne à réfléchir sur le degré de culture numérique des autorités judiciaires dans notre pays. Nous basons ici notre analyse sur le témoignage du principal concerné et de son avocat, ainsi que ceux d'autres hacktivistes, de « technocritiques » et de membres des forces de sécurité. De plus, ont été exploitées des sources primaires telles que des actes judiciaires ou secondaires comme des articles de presse. Sans défrayer la chronique, ce cas a toutefois suscité des interrogations sur : la responsabilité des OIV quant à la sécurisation de leurs ressources numériques ; la puissance d'indexation des moteurs de recherche ; et l'exploitation technique de ces derniers à des fins d'investigation, jusqu'à produire une jurisprudence inédite sur la qualification équivoque du vol « de fichiers informatiques » ou « de données numériques ». Il permet à tout le moins d'illustrer le retard pris dans le traitement par la Justice d'affaires comportant un volet cyber ou en l'occurrence se résumant en totalité à un enjeu de sécurité numérique.

#### a) *D'une navigation sérendipitaire – orientée – à un procès pour vol de données*

En propos préliminaire, il est intéressant de noter que deux procès ont eu lieu en rapport avec l'affaire. L'un a abouti en premier lieu à la relaxe du prévenu et l'invalidation des chefs d'accusation (tribunal de grande instance de Créteil, 2013), l'autre, consécutif, a abouti à la confirmation d'un chef d'accusation pourtant déjugé à Créteil en première instance (cour d'appel de Paris, 2014). Tout commence par la plainte déposée par l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) le 6 septembre 2012, auprès des services de police de Maisons-Alfort (Val-de-Marne) pour « intrusion dans son système informatique et vol de données informatiques.[514] »

[513] Entretien avec l'auteur, 30/03/2023.

[514] https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/. À noter qu'un cas du même type, l'affaire *Kitetoa*, avait mis aux prises en 2002 un journaliste informatique et l'entreprise Tati. Poursuivi pour le même chef d'accusation, ce dernier sera relaxé en appel contrairement à *Bluetouff* (https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-13eme-chambre-jugement-du-13-fevrier-2002/ ; https://www.legalis.net/jurisprudences/cour-dappel-de-paris-12eme-chambre-section-a-arret-du-30-octobre-2002/).

Selon les discussions consignées dans les actes judiciaires, le 3 septembre, l'agence détecte un accès non autorisé sur son serveur extranet[515] sur la base d'une présomption initiale reposant sur la découverte d'un premier puis d'un deuxième articles issus du site *reflets.info*, un média dit alternatif. Ces articles polémiques, qui portent l'un sur les nano-matériaux, l'autre sur des cas de légionellose environnant des centrales nucléaires, s'appuient sur des données exclusives à l'ANSES qui, par extension, sont censées être confidentielles. Ces papiers sont signés de deux pseudonymes dont l'un est « Bluetouff », à savoir le surnom d'Olivier Laurelli, lequel se présente comme un journaliste-citoyen spécialiste d'informatique et peut être considéré comme un hacker. En outre, un fichier tiré de ces données a été attaché en pièce téléchargeable via un hyperlien incorporé dans l'article[516]. Après avoir investigué sur les aspects techniques de la supposée intrusion (journaux de connexion extranet et *logs* d'évènements du pare-feu), l'ANSES délègue *ipso facto* l'enquête à la DCRI (ex-DGSI) du fait de son statut d'opérateur d'importance vitale (OIV). Le service corrobore les éléments apportés par l'agence et acte la présence de documents internes à l'ANSES sur les serveurs hébergeant le site *reflets.info*. Ces documents (8000 pièces[517]) forment un volume total de 8.2Go de données qui ont été téléchargées entre le 27 et le 28 août 2012. L'auteur de ces copies de fichiers se trouve être Olivier Laurelli, lequel a utilisé un moyen d'obfuscation numérique, à savoir ici l'emploi d'un *réseau virtuel privé* plus communément désigné par son acronyme anglosaxon, un VPN.

Notons que ce détail a déjà de l'importance car, plus encore qu'aujourd'hui, l'utilisation de ce type de dispositif, qui ne permet pas tout à fait l'anonymat mais plutôt la confidentialité de sa navigation web, est rare chez les particuliers. Ce logiciel masque en effet l'adresse IP d'un appareil connecté à l'Internet en adoptant celle d'un serveur distant type *proxy* (serveur mandataire) ; dans le cas présent le serveur était basé au Panama. La plupart du temps, les personnes privées ont recours au service d'une entité commerciale disposant de tels serveurs VPN. Or, l'entreprise ici concernée (*toonux.net*) est la propriété d'Olivier Laurelli, alias

[515] Un extranet est l'extension d'un réseau interne à une organisation et ne constitue ni un site internet (accessible au public) ni un intranet (réseau local accessible depuis et à l'intérieur de l'entité aux seuls personnels autorisés). Toutefois, il nécessite une connexion à l'Internet et comporte un dispositif d'authentification à l'adresse des collaborateurs présents à l'extérieur de l'organisation. Aujourd'hui, un VPN constitue le plus souvent ce sas d'accès.

[516] Indisponibles sur la version actuelle du site *reflets.info*, nous avons récupéré lesdits articles via le service *archive.org/wayback-machine* : https://web.archive.org/web/20120831231648/http://reflets.info/nano-argent-risques-dissemination-et-noninformation-du-public/ ; https://web.archive.org/web/20120831194952/http://reflets.info/cas-de-legionellose-a-proximite-des-centrales-nucleaires/

[517] https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-4-chambre-10-arret-du-5-fevrier-2014/. Le chiffre de 7,7Go est parfois mentionné.

« Bluetouff ». Il est donc arrêté et placé en garde à vue le 21 novembre 2012, garde à vue qui va durer trente heures selon le média *Numerama*[518].

Plusieurs chefs d'accusation sont portés contre Olivier Laurelli :

- Accès frauduleux à un système de traitement automatisé de données (STAD), celui de l'extranet de l'ANSES (art.323-1 al.1 du Code pénal, et réprimés par l'art.323-1, al.1, et l'art.323-5) ;
- Maintien frauduleux d'accès dans le STAD (*idem*) ;
- Soustraction frauduleuse de données par leur téléchargement, leurs fixation et enregistrement sur des supports physiques et logiques (disque dur externe, centre multimédia sur le serveur de *reflets.info*) (art.311-1, art.311-3 du Code pénal, et réprimés par l'art.311-3, l'art.311-14, 10, 20, 30, 40, 60).

En première instance, le tribunal de Créteil va accorder le bénéfice du doute à *Bluetouff* pour trois raisons :

- la bonne foi *a priori* d'Olivier Laurelli lorsqu'il déclare être tombé par hasard sur ces données hébergées sur l'extranet de l'agence, par le truchement d'une recherche « naturelle » sur le moteur Google, des mots de son avocat M[e] Olivier Iteanu[519] ; « complexe » selon les mots consignés par les actes judiciaires et prêtés à Olivier Laurelli.
- l'accès libre au répertoire contenant les données considérées ne disposait d'aucun dispositif de protection logique (authentification par identifiants et mots de passe) ;
- l'ANSES a convenu qu'elle était responsable d'une défaillance technique, et qu'aucune faille n'a été exploitée « sans procédé de type "hacking".[520] » Un tel dispositif était bien présent mais placé seulement au niveau de la racine du serveur et ainsi de la page d'accueil de l'extranet. L'ANSES n'a donc pas clairement manifesté l'intention de restreindre l'accès à ce répertoire aux seuls usagers de l'agence et convient de son manquement.

[518] https://www.numerama.com/politique/28295-bluetouff-condamne-en-appel-pour-avoir-su-utiliser-google.html
[519] Interview d'Olivier Iteanu, chaine *Thinkerview*, 13/03/2014.
[520] https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/

Le 23 avril 2013, le tribunal relaxe donc Olivier Laurelli et invalide les deux premiers chefs d'accusation (accès et maintien frauduleux). Quant au troisième, il va – du moins officiellement – être à l'origine du revirement de la Justice.

Effectivement, la cour d'appel de Paris va reprendre et invalider le premier jugement un an plus tard, en février 2014. Les trois chefs d'accusation sont repris mais c'est bien le dernier sur lequel se cristallisent toute l'attention et la controverse, comme nous allons le voir. Un changement de tonalité dans la terminologie même des protagonistes judiciaires peut du reste être observé. Ainsi, on ne parle plus de « *défaillance technique* » mais de « *faille de sécurité* » ou encore non plus de « *documents* » ou « *données informatiques* », mais de « *données litigieuses* »[521]. À ce stade, deux chefs sont retenus : Olivier Laurelli est coupable non d'avoir accédé au STAD[522] de l'ANSES mais d'y avoir maintenu un accès frauduleux. Ce qui paraît assez contradictoire sur un plan technique et pratique, car il faut bien accéder à un SI en première action si l'on souhaite y maintenir un accès. C'est ce que pointe à raison Me Iteanu dans un tweet :


Source : capture Twitter/X [523].

Mais d'un point de vue juridique, c'est ce qui a été retenu. Précisément, le deuxième chef d'accusation a porté sur ce que l'on pourrait appeler par analogie la technique du « pied-dans-la-porte informatique ». En l'espèce, on impute à Olivier Laurelli l'intention de profiter de la faille de paramétrage de l'extranet car il a procédé à une *énumération* des répertoires du serveur jusqu'à remonter à sa racine et, dès lors, constaté la présence de contrôles d'accès. Or, bien que ce ne soit visiblement pas porté à la connaissance des magistrats, en qualité de hacker, *Bluetouff* n'était pas censé ignorer ce qu'il faisait. C'est ce qui lui est toutefois reproché indirectement quand il est fait mention du fait qu'il avait « *conscience de son maintien irrégulier* » dans le STAD visité, « *où il a réalisé des opérations de téléchargement de données à l'évidence protégées*.[524] »

[521] https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-4-chambre-10-arret-du-5-fevrier-2014/
[522] Aujourd'hui, on emploie plus certainement l'expression système d'information, même si celle-ci est moins précise et moins focalisée sur l'aspect technico-informatique que ne l'est le STAD.
[523] https://twitter.com/search?q=from%3Aiteanu+%22bluetouff+relax%C3%A9%22&f=top. Nous avons reproduit un tweet postérieur, dont voici l'originel : https://twitter.com/iteanu/status/431115509325516800
[524] https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-4-chambre-10-arret-du-5-fevrier-2014/

Enfin, revenons à la source de la polémique. Le dernier chef d'accusation charge donc Olivier Laurelli d'avoir volé des données numériques. Ainsi, jusque-là, les sources du droit et notamment la législation faisaient défaut quant à l'application de la qualification de vol aux données, puisque le Code pénal le définissait comme « *la soustraction frauduleuse de la chose d'autrui* » en vertu de l'article 311-1. Or, la controverse a porté sur la notion de chose qu'on assimilait à un objet tangible ; ce qui n'est pas le cas avec des données par nature immatérielles. L'on peut raisonnablement penser que le juge du tribunal de Créteil a estimé ne pas être en mesure d'user de son pouvoir normatif dans l'extrapolation dudit article du Code pénal, par défaut d'une législation adéquate[525]. Ce dont s'est arrogé en revanche et visiblement le magistrat de la cour d'appel de Paris en procédant à une interprétation de la loi. Maître Iteanu et son client feront appel du jugement mais il sera confirmé le 5 février 2014, et Olivier Laurelli débouté de son pourvoi en cassation le 20 mai 2015[526].


Source : capture sur Twitter/X [527].

Entre temps, dans le cadre du renforcement des dispositions relatives à la lutte antiterroriste et précisément dans l'article 16 consacré à la lutte contre la contrefaçon[528], l'article 323-3 est modifié pour prendre en compte la source jurisprudentielle ressortant à l'affaire *Bluetouff*. Un délit spécifique est alors reconnu pour qualifier le vol de données, dont leur reproduction frauduleuse. En d'autres termes, copier des données, c'est les voler, et cette caractérisation vient consacrer *a posteriori* le jugement de l'affaire *Bluetouff*. Compte tenu de la technicité juridique du dossier, nous n'entrerons pas davantage dans les détails, mais il faut tout de même noter que cette nouvelle loi relancera la controverse notamment doctrinale afférente à l'affaire. Aujourd'hui, à l'ère des intrusions informatiques, des fuites et vols de données quasi quotidiennes, il paraît normal de statuer sans tergiversation sur ce type de cas, mais en 2012-2015, la chose est moins évidente. D'ailleurs, s'il y a bien eu inflation de la jurisprudence autour des accès frauduleux dans des STAD, avec des affaires en 2017 et 2018

[525] L'on pourra se référer à cet acte de colloque très riche sur cette réflexion (https://www.senat.fr/colloques/office_du_juge/office_du_juge9.html).
[526] https://www.legifrance.gouv.fr/juri/id/JURITEXT000030635061/ Il est condamné à verser une amende de 3000 euros et la décision sera inscrite dans son casier judiciaire.
[527] https://twitter.com/search?q=from%3Abluetouff+%22c%27est+%C3%A9norme+je+suis+officiellement%22+&f=top
[528] https://www.legifrance.gouv.fr/loda/id/LEGIARTI000029755281/2014-11-15#LEGIARTI000029755281

notamment, il demeure néanmoins un flou juridique lié à la puissance d'indexation de technologies qui sont la propriété d'entreprises systémiques comme les GAMAM[529].

En l'occurrence, selon les propos de Me Iteanu, le groupe Google (Alphabet aujourd'hui) n'a pas été cité ni auditionné y compris dans le cadre de l'enquête menée par la DCRI[530]. Or, c'est bien l'indexation et donc la publicisation des données de l'ANSES qui a permis à Olivier Laurelli d'accéder à l'extranet de l'agence. À cet égard, un point intéressant n'apparait pas dans les actes judiciaires. S'il est admis au bénéfice du doute accordé au journaliste-hacker qu'il est tombé par erreur sur l'extranet de l'agence, *id est* par sérendipité, il a toutefois évoqué auprès de la DCRI l'emploi d'une « recherche complexe » sur le moteur américain. En langue profane, l'on pourrait penser qu'il a utilisé de simples mots-clés, comme tout internaute est habitué à le faire quotidiennement. Toutefois, la très grande majorité des gens ignorent les potentialités des moteurs en termes de recherche avancée. En l'occurrence, Olivier Laurelli a utilisé ce qu'il est convenu d'appeler des *dorks* dans le jargon de l'OSINT et plus globalement dans le monde de la cybersécurité. Popularisée par un hacker américain, Johnny Long[531], cette syntaxe particulière fondée sur des opérateurs spécifiques autorise tant une précision qu'une discrimination sémantiques chirurgicales dans les recherches sur les moteurs. Autrement dit, on allège considérablement le bruit numérique en orientant, si l'on peut dire, les œillères des logiciels qui opèrent le rapatriement des résultats d'un moteur de recherche. Tous ces derniers sont sensibles à la plupart des *dorks* avec des nuances, Google étant le plus efficace et permissif. Florent Curtet[532], hacker de son état, ou encore Bernard Dousset, spécialiste de *data-mining* parlent des *dorks* en des termes significatifs, les présentant comme un outil *« très puissant* »[533]. Les *dorks* peuvent en effet être utilisés à des fins de recherche (précision dans les requêtes, productivité) mais aussi dans un but défensif (RSSI cherchant des failles de sécurité sur leurs propres SI) ou offensif (identifier ces mêmes vulnérabilités chez une cible), dans le cadre de stratégies d'investigations en renseignement ouvert (OSINT) ou de « reconnaissance passive » si l'on adopte le vocabulaire des hackers.

Si ces détails terminologiques ne sont pas mentionnés par les greffiers, c'est parce qu'ils s'accompagnent d'autres incompréhensions chez les magistrats des tenants et aboutissants techniques de l'affaire.

---

[529] Nous renvoyons ici au bilan effectué par un cabinet d'avocats (https://info.haas-avocats.com/droit-digital/laffaire-bluetouff-la-consecration-du-vol-de-donnees-informatiques#_ftn2)

[530] Interview d'Olivier Iteanu, *op. cit.*

[531] Ce dernier a créé un site web légal mais qu'on peut qualifier de « gris », accessible sur le « web surfacique » et qui référence une base entière de *dorks* (très tendancieux) prêts à l'emploi. Nous ne le mentionnerons pas ici. Voir Johnny Long, *Google Hacking. Mettez vos données sensibles à l'abri des moteurs de recherches*, Dunod, 2005, 350 p. S'ils nécessitent une certaine « gymnastique » d'usage, ces opérateurs sont accessibles – certes dans une version très limitée – via une page tout à fait quelconque : https://www.google.com/advanced_search.

[532] Entretien avec l'auteur, 30/09/2021.

[533] Entretien avec l'auteur, 11/07/2017.

### b) *Clé de lecture du cas d'étude*

L'affaire *Bluetouff* nous éclaire sur les difficultés pour les autorités, ici judiciaires, à appréhender les lois informelles et codes de l'espace numérique. Comment expliquer, en effet, le revirement de la Justice, le fait qu'Olivier Laurelli soit relaxé puis condamné, de surcroît pour un maintien subséquent et non son accès frauduleux puis finalement un vol de données sans fondement législatif incontestable (extraction immatérielle égale soustraction d'un objet[534]) ? Le montant de l'amende dit aussi quelque chose de ce bégaiement judiciaire puisqu'on est loin d'une sentence maximale, à l'époque élevée à deux ans et 30 000€[535]. S'agit-il d'un acharnement judiciaire comme l'a laissé entendre Olivier Laurelli et le suggèrent également policiers et spécialistes que nous avons interrogés ? Ou de l'inadaptation manifeste d'un corpus législatif carencé face à un temps technologique particulièrement rapide ? L'affaire aura eu en tout cas le mérite de consacrer la notion de vol de données.

- ***Disposition mentale – 1ère caractéristique : la complexité du réel et du « village global »***

Il est coutume de dire que le temps médiatique n'est pas le temps politique qui n'est pas le temps judiciaire. S'ils propulsent justement la communication médiatique, les progrès technologiques sont tels qu'il en va d'un autre degré de vitesse, fulgurant celui-ci. La culture iconoclaste des hackers est aux avant-postes de cette pression technologiste. Dans une telle optique, un moteur de recherche, comme tout autre dispositif logiciel notamment est à décortiquer, contourner, détourner. Surtout quand on cherche à connaître les coulisses du pouvoir. C'est en somme ce qu'a réalisé Olivier Laurelli en usant de la technique des *Google dorks* aussi appelée *Google hacking*. Le slogan du site *reflets.info* l'exprime sans détour : *Bluetouff* pilote un « journal d'investigation en ligne et d'information-hacking », un *bateau pirate* de l'information alternative qu'on assimile parfois à de la presse ré-informative. C'est bien le jeu et l'enjeu actuels de la libéralisation de l'info-communication. Or, ces « francs-tireurs » du journalisme citoyen ont souvent raison des postures traditionnelles de l'État au point de le déstabiliser[536].

Désemparée, l'ANSES l'est également quand lui sont subtilisés ces nombreux documents à caractère confidentiel. Comment un simple moteur de recherche a-t-il conduit à une forme de piratage involontaire ? La Justice le précise : il n'y a pas eu usage de procédé de type

[534] Voir l'avis de l'avocat général de la Cour de cassation rapporté par le journaliste Marc Rees : https://www.nextinpact.com/article/18067/95165-affaire-bluetouff-cour-cassation-consacre-vol-fichiers-informatiques

[535] Aujourd'hui portée à trois ans et 100 000€.

[536] Voir par exemple Emmanuel Bloch, *Communication de conflictualité et mouvements activistes sur Internet*, *passim.* ; ou Nicolas Moinet, *Les sentiers de la guerre économique*, T2, *op. cit.*, pp. 91-101.

« hacking ». Mais, au-delà de la dimension illicite du procédé, les autorités judiciaires savent-elles du moins de quoi il est question ? C'est qu'elles jugent l'affaire *Bluetouff* sur fond de profonde méconnaissance du monde numérique. Si Me Iteanu juge que les magistrats n'ont pas forcément à être des experts du sujet ou des « geeks », il pointe toutefois les flagrants manquements des acteurs judiciaires et leur « distance » vis-à-vis des sujets cyber[537]. D'après l'avocat, si l'ensemble de la profession journalistique n'en a fait qu'un traitement superficiel, la presse spécialisée quant à elle fulmine et s'émeut de la condamnation. Surtout, elle s'inquiète d'un précédent pouvant remettre en cause la liberté d'information. En outre, le journal d'investigation Mediapart publie un article sarcastique reprenant les déclarations officielles du procès, avançant que les magistrats étaient « *totalement hermétiques à toute notion technique, même les plus basiques*. »

> « *En ouverture d'audience, la magistrate chargée de rappeler les faits semblait même ne pas connaître Google, prononcé à la française "gogleu", ni savoir ce que signifie un "login", prononcé "lojin". Difficile, dans ces conditions, d'expliquer qu'il est effectivement possible de tomber sur des documents de travail par une simple recherche… "Mais il faut tout de même taper des mots-clés…", demande ainsi, dubitatif, un des juges. "Comment faites-vous pour arriver sur des questions de santé publique alors que vous cherchiez des choses sur la Syrie ?" Au fil de l'audience, on se rend compte que les magistrats ont une vision totalement fantasmée d'internet, et des documents que l'on peut y trouver… "Vous ne vous souci*[i]*ez pas de savoir si vous alliez tuer toute la planète ?" s'indigne ainsi une magistrate alors que l'accusé vient de lui expliquer que ces documents n'étaient, visiblement, pas confidentiels.* […] *Le parquet, dont le représentant a confirmé à l'audience qu'il n'a "même pas compris la moitié des termes que j'ai entendus aujourd'hui", avait choisi de poursuivre coûte que coûte. Au nom de la mauvaise foi : "Vous saviez que cet extranet était normalement protégé".*[538] »

Reste une question : si désormais plus de 80% des affaires pénales ont un volet cyber, comment expliquer le fait qu'il y ait « *malheureusement très peu de juges spécialisés dans le cyber*.[539] » On peut ainsi estimer qu'un dialogue de sourds s'est joué lors des deux procès, entre un monde judiciaire à la peine dans sa compréhension des codes du cyberespace, et un

[537] Interview d'Olivier Iteanu, *op. cit.*

[538] Cité par *Numerama,* https://www.numerama.com/politique/28295-bluetouff-condamne-en-appel-pour-avoir-su-utiliser-google.html

[539] Entretien avec Guillaume Poupard, 17/04/2023. Le N-TECH et adjudant-chef Stéphane Tonelli parle en 2017 d'un seul magistrat expert des TIC, Emmanuelle Legrand (entretien avec l'auteur, 28/06/2017). Il apparaît qu'en date de juillet/août 2022 « *trois magistrats seulement traitent les dossiers de cybercriminalité en France alors que le nombre d'attaques augmente à un rythme exponentiel depuis deux ans* » et qu'un parquet national cyber, préconisé depuis au moins 2021, n'a pas encore vu le jour (https://www.senat.fr/basile/visio.do?id=qSEQ220700681&idtable=q397252|q417232&_c=%22parquet+national+cyber%22&rch=gs&de=20030909&au=20230909&rqg=drqscpt&dp=20+ans&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn).

« journaliste-citoyen-hacker » dont les usages et la manière de penser ne cadrent certainement pas avec cette situation de communication ou plutôt d'incommunication.

- ***Disposition mentale – 2e caractéristique : culture de l'intelligence rusée***

{site:gouv.fr filetype:pdf confidentiel OR secret OR inurl:"index of"} Tel pourrait être formulé le début d'une requête – contestable – de type *dork*, consistant ici à trouver les mentions « confidentiel » ou « secret » sur des documents de format PDF issus de sites gouvernementaux français ou les index racines de mêmes sites web[540]. Complexe pour le profane mais à la portée de tous, cette requête effleure pourtant à peine les possibilités à caractère invasif autorisées par les moteurs de recherche. La question est de savoir si, à travers ce type de recherche avancée, l'on peut se rendre coupable de piratage d'un SI. On retrouve ici toute la philosophie de court-circuitage des machines et technologies relative aux hackers. Parmi les caractéristiques fondamentales de ces derniers se trouvent en bonne place l'anticonformisme et la créativité. C'est donc user d'intelligence et de ruse que de les pousser à leurs limites. À l'instar de bon nombre d'observateurs, l'ancien directeur de l'ANSSI, Guillaume Poupard, regrette la tournure qu'a prise l'affaire. « *À l'ANSSI,* dit-il, *dès le début on avait des plaintes déposées pour des scans de ports. C'est exagéré. Aujourd'hui, il y a une meilleure compréhension du sujet malgré tout.*[541] » De même, certains policiers vont porter un avis critique sur le traitement de l'affaire et celui appliqué à son prévenu.

- ***Disposition mentale – 3e caractéristique : le triptyque patriotisme–unité–souveraineté***

En effet, des policiers de la DGSI vont déplorer l'acharnement dont le prévenu a fait l'objet : « *On a perdu notre temps avec Olivier Laurelli.* » Ce dernier a du reste gardé le contact avec deux anciens officiers du service avec qui il avait de bonnes relations[542]. De son côté, Fabrice Epelboin dénonce l'acharnement judiciaire de sept ans qu'a subi *Bluetouff*, de qui il est une connaissance. Il évoque par ailleurs le fait que cela a pu avoir un lien avec ce qu'il appelle les « réseaux Sarkozy », du nom de l'ancien chef d'État. Effectivement, Olivier Laurelli avait déjà été inquiété par la Justice pour des faits mineurs et en l'espèce son traitement médiatique

[540] En l'occurrence, *Bluetouff* couvrait le conflit syrien et avait l'habitude d'utiliser le *dork* « site:*.gov.sy » jusqu'au moment où, dit-il, il a oublié d'inclure ce paramètre dans ses requêtes (entretien avec OL). Les sites gouvernementaux syriens ont été particulièrement attaqués à cette époque, notamment par les *Anonymous*.
[541] Entretien avec l'auteur, 17/04/2023. Les ports dits logiciels sont des interfaces (ouvertes ou fermées) permettant le fonctionnement de processus/services sur un système informatique. Ouverts, ces ports prêtent potentiellement le flanc à des attaques.
[542] Entretien avec l'auteur, 30/03/2023.

concernant les liens que l'ancien président entretenait avec la Lybie[543]. Toujours selon Fabrice Epelboin, les documents copiés sur le site de l'ANSES avaient trait à des questions politiques sensibles relatives à Martine Aubry.

Cette affaire est-elle le signe d'une incohésion manifeste entre les différents organes de l'État ? La question mérite d'être posée et, selon Fabrice Epelboin, « *elle est représentative des intérêts et de la sanctuarisation de l'État français*.[544] » Dans cette perspective, l'avocat d'Olivier Laurelli stigmatise les atteintes aux libertés individuelles que portent la Loi de programmation militaire 2013 (LPM) et ses dispositions connexes (loi sur la géolocalisation de suspects sans contrôle judiciaire). On le voit, et indépendamment des intérêts propres à chacun des acteurs de l'affaire et de son contexte, il est difficile d'y voir une unité de vision au sein des institutions de l'État, entre la DGSI qui semble minimiser sa gravité, l'ANSSI qui ne se prononce pas à l'époque, des autorités politiques qui ne prennent guère part au débat, et une Justice enfin qui, dans une posture particulièrement inconfortable, tente de faire au mieux son travail mais accuse un certain déphasage avec son époque. Élément notable par ailleurs, à aucun moment pour le premier comme le deuxième procès, l'ANSES ou toute autre entité ne se constituent parties civiles. Ce qui dénote un certain malaise car, bien que l'agence reconnaisse une erreur de sécurisation, il ne s'agit pas encore d'une faute au regard de la législation encore limitée de l'époque. Aujourd'hui, que se serait-il passé compte tenu de l'avènement du Règlement général de protection des données (RGPD) en mai 2018 ? Si l'usage de données à caractère personnel (ici : informations sur Martine Aubry ?) avait été impliqué, l'ANSES aurait vraisemblablement été considérée elle aussi fautive et l'objet d'une sanction. Du moins en vertu des dispositions du Code de la défense[545].

Enfin, en filigrane de l'affaire s'est joué un rapport de force diffus qui est aujourd'hui encore plus problématique ou du moins plus évident pour la France et ses partenaires européens. Cela concerne la question d'un degré de responsabilité quelconque du groupe Alphabet dans la mise à disposition de données privées. Ce dernier a-t-il été inquiété pour la capacité d'indexage des contenus web dont fait preuve son moteur de recherche bien connu ? Les discussions lors des procès ont-elles du moins donné lieu à cette réflexion ? L'avocat spécialisé dans le droit des TIC qu'est M[e] Iteanu s'est très tôt posé la question en rappelant l'affaire Snowden et le fait que les GAFAM à travers *PRISM* et ses suites ont atteint le degré le plus avancé de la surveillance de masse. Même si les possibilités du moteur américain sont ouvertes à tous, le monopole commercial et d'usage européen de Google ne fait aucun doute.

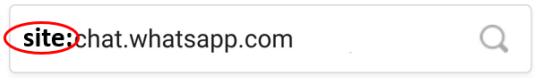
[543] C'est l'affaire « Amesys », du nom de cette ancienne société de services d'ingénierie informatique qui a conçu et vendu au colonel Kadhafi le logiciel d'interception de communications électroniques baptisé *Eagle*.
[544] Entretien avec l'auteur, 08/04/2022.
[545] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000028345141. La dernière version de l'article date de décembre 2013, soit entre les deux procès.

Le fait de ne pas avoir soulevé cette question montre la frilosité, l'inconscience voire l'incohérence des autorités en général face au fonctionnement des moteurs de recherche comme Google en termes d'indexation et de restitution publique de ressources potentiellement sensibles. En somme, le messager à qui l'on s'en prend est-il Olivier Laurelli ou Google ? Il semble aujourd'hui acquis qu'on ne tire pas sur le – simple – messager Google, la loi du « progrès » technologique suivant son cours.

Notons tout de même que le traitement fait ici à Google, qui n'aura fait l'objet d'aucune sollicitation dans le cadre de l'instruction ni de l'enquête, s'est avéré bien différent dans d'autres cas. En particulier, le déréférencement des ressources de l'extranet de l'ANSES a-t-il été réalisé ou ces dernières sont-elles restées accessibles pendant et après le jugement ? La réponse est vraisemblablement négative, et c'est l'agence qui a dû se charger d'en interdire l'accès. Une affaire advenue en février 2020 est éclairante à ce sujet, celle de l'application *Whatsapp* appartenant au groupe Meta. Plusieurs mois avant, un journaliste allemand, Jordan Wildon, informe l'entreprise de March Zuckerberg que les liens des groupes privés de la messagerie instantanée sont référencés sur plusieurs moteurs de recherche dont le plus utilisé en Occident, Google. Sans succès, Meta ne daignant répondre à un individu isolé. Autrement dit, les moteurs indexent les accès privés de *chatgroups* normalement protégés par leur URL encodée. En effet, lorsqu'on crée un tel groupe, est alors généré un lien que l'on peut partager aux personnes autorisées. Par la négligence de Facebook/Meta, ces liens ont été automatiquement moissonnés-indexés par les moteurs de recherche, permettant à n'importe qui de pouvoir s'infiltrer dans des centaines de milliers de groupes privés[546]. Détail qui a son importance, tomber sur une telle URL était absolument fortuit (du fait de la complexité du lien, doté de caractères aléatoires. Ex. : */CDZlwwg1LdX2B2yfOwrDi*). En revanche, utiliser un *dork* ("site:") très basique permettait d'avoir un accès direct au référencement de toutes les URLs de groupes. C'est ce qu'a fait le journaliste qui, échaudé, contacte les médias allemands, lesquels répercutent rapidement l'évènement auprès de leurs homologues européens. Cette fois, le scandale mobilise Facebook qui s'empresse de demander le déréférencement auprès notamment de Google. Bien trop tard. Bien sûr, en position d'outsiders, plusieurs moteurs étrangers (le russe Yandex…) ou promouvant la confidentialité (DuckDuckGo…), vont profiter de la situation et délibérément tarder à opérer ce retrait. Google, pour sa part, sera le plus rapide, en dépit de sa réponse initiale, à la fois gênée et condescendante vis-à-vis de Meta.

[546] Voir cet article documenté https://www.blogdumoderateur.com/whatsapp-conversations-privees-indexees-google/. Les liens générés ressemblent à celui-là : « https://chat.whatsapp.com/CDZlwwg1LdX2B2yfOwrDi ». À l'époque, nous avions personnellement pu vérifier le nombre de groupes privés indexés auprès du moteur Bing de Microsoft, qui avait été moins rapide que Google à les déréférencer. Il y en avait 697 000.

Plusieurs groupes seront alors infiltrés en France, par des journalistes de *Numerama* par exemple, qui accèderont aux conversations de plusieurs personnalités politiques[547].




*Simulation de requête utilisée par Jordan Wildon (grâce au dork* "site:"*)* (capture personnelle)

L'ANSES n'a certainement pas reçu de tels égards de la part d'Alphabet. Pourtant, loin d'être un État et la conséquence d'une injonction judiciaire, c'est un « simple » individu qui par le levier médiatique a fait basculer la situation.

- ***Dispositif opérationnel – 4e caractéristique : l'information au centre du jeu stratégique***

Quel enseignement tirer ici de l'affaire *Bluetouff* ? Au vu, d'une part, de la démonstration de la méconnaissance criante des autorités judiciaires en termes de culture numérique, d'autre part de la non prise en considération de l'importance de l'outil informationnel pourvoyeur (le moteur Google), il est loisible de penser que l'information n'est pas perçue comme stratégique. Pourtant, cette dernière est bien au cœur de l'affaire : un individu emploie une technologie spécialisée dans la recherche qui va le mettre en relation technique avec les serveurs d'un réseau informatique et lui permettre d'en exfiltrer des données.

Dans un autre registre, axé sur les droits des justiciables, l'ancien policier repenti de la DGSI, Cédric D., dit « Haurus », a porté à la connaissance du grand public des éléments inédits et polémiques sur la question des analyses forensiques réalisées dans le cadre des enquêtes policières comportant un volet cyber. Selon ce dernier, il existe une asymétrie manifeste dans la maîtrise de ces analyses sur les appareils de téléphonie mobile. Un avantage qui serait au bénéfice des policiers et aux dépens des avocats et magistrats dans les conclusions réelles qu'on pourrait tirer du traitement des pièces numériques constitués par la police (exploitation des interceptions de communications, données enregistrées…). En 2021, il publie un ouvrage plaidant la cause où il confie : « *On peut faire dire n'importe quoi à la téléphonie dans une enquête, qu'on présente comme une preuve irréfutable* », expliquant que son livre « *s'adresse à tous les acteurs de la procédure, avocats et mis en cause certes, mais aussi magistrats et*

[547] https://www.numerama.com/tech/607210-sur-google-on-trouve-en-un-clic-des-milliers-de-numeros-francais-lies-a-whatsapp.html. En ajoutant des mots-clés spécifiques/thématiques aux liens, on pouvait alors espérer retrouver certaines personnes.

*enquêteurs intéressés à la problématique. Tout le monde doit avoir les mêmes armes lorsque l'on fait face à la justice.*[548] »

- ***Dispositif opérationnel – 5e caractéristique : maîtrise de l'information via le triptyque acquisition–sécurité–influence***

L'affaire Laurelli nous apprend que l'ANSES fait de la veille notamment d'opinion/réputation en ce début de décennie 2010. Rien d'exceptionnel en soi pour une agence publique aussi exposée, à moins qu'il s'agisse, là aussi, du fruit de la sérendipité dans le cadre du travail d'un chef d'unité du service[549]. C'est en effet ce dernier qui a trouvé mention des données copiées et reportées dans l'article publié par *Bluetouff*. Sans cette coïncidence ou cette veille toutefois, l'affaire n'aurait peut-être jamais vu le jour. Au-delà de l'anecdote, il est surtout intéressant de pouvoir apprécier les manquements à la sécurité numérique d'un OIV tel que l'ANSES. Concédons toutefois que si la détection de failles applicatives Web est encore trop commune de nos jours, ce type de négligence informatique était encore plus habituel à l'époque. À cet égard, le contexte de ce début de décennie est déjà particulièrement inquiétant puisque l'affaire *Bluetouff* fait écho à celles des « intrusions » et « vols » de données similaires ayant touché notamment France Télévisions, Areva, les services de Bercy ou encore feu l'entreprise Tati.

Par ailleurs, s'agissant toujours de sécurité numérique, on peut préciser quelques éléments relatifs aux techniques de hacking via un simple moteur de recherche. Comme nous l'avons mentionné plus haut, lorsque Olivier Laurelli accède aux données de l'ANSES, il le fait en remontant l'arborescence des répertoires de l'extranet. Dans le jargon du *pentesting*, on appelle cela du *dirbusting*, à savoir de la « destruction de répertoires ». Cela peut se faire soit par le biais d'outils automatisés, soit assez simplement en modifiant manuellement une URL ; par exemple en devinant la carte d'un site web et le nom des dossiers dans un serveur. On peut aussi assimiler le *dirbusting* à une forme de *latéralisation*, technique employée pour cartographier des réseaux informatiques et approfondir une intrusion dans un SI. Il semble d'ailleurs que ce soit ce qui ait perdu le principal concerné puisqu'il a avoué de bonne foi aux enquêteurs avoir procédé à cette technique.

De plus, si cela n'a pas de rapport direct avec l'affaire, il est utile de préciser que d'après leur propre témoignage, des officiers de la DGSI utilisent l'application de messagerie

[548] Cité par Jean-Marc Manach, https://www.nextinpact.com/article/45437/haurus-dgsi-aux-droits-defense-en-passant-par-darkweb. « Haurus », *Investigations & téléphonie mobile : le guide à l'usage des avocats*, Hachette, 2020, 183 p.

[549] https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/

*Whatsapp* dans le cadre de leur activité régulière et de filatures pour une meilleure coordination[550]. Si la direction du service leur en a bien interdit l'usage en vertu des impératifs classiques et nécessaires d'hygiène numérique, ces derniers y dérogent sans avoir *a priori* bien conscience du fait qu'il s'agisse d'un outil américain, qui plus est fortement déconseillé par les meilleurs spécialistes de cryptographie, leur préférant *Signal* ou encore, pour des raisons souveraines, *Olvid*. En mai 2022, l'unité du RAID a d'ailleurs adopté officiellement cette messagerie instantanée française. Gageons que tous les autres services de sécurité fassent de même. S'il ne s'agit probablement pas de policiers spécialisés dans le cyber, ces officiers de la DGSI montrent en revanche une certaine innocence, évoquant par exemple faire bien attention de supprimer les messages et groupes *Whatsapp* en fin de journée. Si quelques doutes subsistent déjà sur le chiffrement supposé de bout-en-bout de l'application (son code source est privateur), on connait du moins aujourd'hui les très nombreuses métadonnées que collecte Meta à travers elle[551]. Et il va sans dire que les données supprimées localement (sur les appareils et l'application) ne le sont pas en accès distant sur les serveurs de Meta…

Enfin, pour revenir à l'affaire proprement dite, on peut noter le changement de posture de l'ANSES quant aux autorisations d'indexage de son site web par le moteur Google. Le changement intervenant très tôt par suite de l'affaire *Bluetouff*. Les informaticiens ou webmestres connaissent en général très bien l'opération consistant à placer à la racine d'un site web un fichier de non-indexage (*no index*) ou un fichier qui par convention sera baptisé *robots.txt*. Tout internaute peut consulter le degré de protection théorique d'un site à l'indexage en ajoutant à son URL le chemin vers le fichier-ressource (ici pour l'ANSES) : *https://www.anses.fr/robots.txt*. Théorique, car il n'y a aucune obligation contraignante à interdire cet indexage aux moteurs. Comme souvent dans la gouvernance de l'Internet, il s'agit plus d'une convention que d'une disposition légale. Or, précisément fin août 2012, la politique d'indexage mentionnée à l'adresse des *crawlers* des moteurs de recherche est somme toute assez limitée. Ci-dessous, des captures d'écran figurent la politique d'indexation du site de l'ANSES au 27 août 2012, date à laquelle Olivier Laurelli accède à l'extranet, et au 22 février 2013, le jour exact où cette politique a été modifiée par l'agence[552]. Nous avons tiré ces captures de la *Wayback Machine* depuis le site *archive.org*.

[550] Alex Jordanov, *Les guerres de l'ombre de la DGSI - Plongée au cœur des services secrets français*, Nouveaux mondes Éditions, 2019, 296 p., pp. 289-290. Leurs conversations de groupes privés auraient pu être infiltrées compte tenu de l'affaire que nous avons narrée précédemment.

[551] À l'origine, *Whatsapp* est une fork (une déclinaison libre de droit) du cryptosystème de *Signal*. Pourtant, Facebook/Meta ajouta une brique logicielle propriétaire/fermée peu après le rachat de l'application à deux jeunes Américains en 2014, pour la somme de 19Mds$.

[552] https://web.archive.org/web/20120827112127/http://www.anses.fr/robots.txt (27/08/2012). Un *crawler* est un robot indexeur. Par exemple, celui de Google s'appelle *GoogleBot*. La politique d'indexation au cours de l'affaire : https://web.archive.org/web/20130222085650/http://www.anses.fr/robots.txt (le 22/02/2013).

```
User-agent: *
Disallow: nojs.htm
Disallow: js.js
Disallow: jsa.js
Disallow: jsb.js
Disallow: css.css
Disallow: blank.htm
Disallow: /PICT/
Disallow: /PICT2/
Disallow: /Documents/
Sitemap: sitemap.xml
```

*Politique d'indexation au 27/08/2012*

```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
Disallow: /sites/default/files/documents/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

*Politique d'indexation au 22/02/2013*

On peut donc en conclure que la leçon a été bien comprise de la part de l'ANSES, qui a pris des mesures assez rapides. On peut remarquer sur la deuxième capture la mention explicite de non-indexation de répertoires soit plutôt anodins, soit plutôt sensibles, comme ceux liés à des requêtes d'accès aux dossiers contenant les mots de passe ou des fichiers de paramétrage ou d'actualisation/mise à niveau (*update/upgrade*) où des contenus d'informations peuvent être laissées et donc collectées par un attaquant. Enfin, la mention « user-agent : * » signifie qu'on n'autorise théoriquement aucun *crawler* de moteur ou autre dispositif de moissonnage à indexer ces contenus.

- ***Dispositif opérationnel – 6e caractéristique : processus réticulaire via un dispositif intelligent***

Bien entendu, il n'est guère question dans le cadre du procès d'une collaboration entre un hacker et les autorités, mais plutôt du contraire. Olivier Laurelli est avant tout considéré comme un activiste, avant même d'être un hacker. En fait, il est bien un *hacktiviste* car il allie

compétences techniques et engagement idéologique : entrepreneur en infogérance, informaticien autodidacte, et journaliste-citoyen d'investigation politique. Aux États-Unis, on le qualifierait probablement de *muckracker*[553], journaliste-justicier en quête de divulguer des scandales d'État ou privés. Or, comme l'avancent certains observateurs, ces profils sont très performants pour mettre au jour des informations grises ou noires. Sans parler de réseau à même de produire des connaissances globales, *Bluetouff* est bien en contact avec certaines autorités de l'État, en l'espèce les services de renseignement. Fabrice Epelboin évoque le lien de ce dernier avec la DGSE, du fait de sa maîtrise de sujets internationaux et de la richesse de ses réseaux humains sur plusieurs théâtres extérieurs qui pouvaient intéresser l'État français (Syrie, séquence des *Printemps arabes*, Maghreb, Lybie…). En outre, il souligne « *l'arrestation de façade* » à laquelle la DGSI s'est prêtée lorsqu'Olivier Laurelli a été appréhendé[554].

> « *Il y a des contacts avec les services de renseignement étatiques parce qu'il y a beaucoup de patriotes chez les hackers, mais c'est difficile à structurer car on passe juste par des individus*. […] *La question du hacking et des hackers n'est pas binaire : il n'y a pas de "gentils" ou de "méchants" hackers. Il faut aller chercher l'intelligence, le savoir-faire, entre les deux : chez les hackers gris dits "hacktivistes". Ils ne respectent pas nécessairement la loi mais ils sont très compétents, et donc utiles pour le renseignement et ont de ce fait des contacts avec les services*. […] *Il était respecté à la DGSE*.[555] »

En particulier, il aurait été mis en relation avec la direction technique du SR extérieur. Si le principal concerné reste discret, il confirme les propos mais dit ne jamais avoir été investi de quelque mission confiée par les autorités. « *L'État ne m'a jamais confié de missions malgré mes "entrées"*.[556] » Parmi ses réseaux, certaines personnes ont toutefois été contactées dans cette optique, mais elles ont décliné. Quant à la DGSI, il était comme on l'a dit en rapport très distant avec la DCRI à l'époque, et a gardé le contact avec deux anciens officiers désormais retraités.

Ces contacts intéressés et finalement peu constructifs au regard de notre clé de lecture des évènements font peu de doute : aucun réseau sérieux n'a été établi au-delà des interactions ponctuelles et parfois litigieuses. Ironie du sort, Olivier Laurelli a travaillé indirectement pour le compte de la présidence de la République puisqu'une des entreprises qu'il a cofondées, Bearstech, a été un temps en charge de l'hébergement des données de l'Élysée. De son propre aveu, « l'affaire Bluetouff » aura collé à la peau d'Olivier Laurelli en entachant sa réputation, et lui nuit toujours aujourd'hui.

[553] Que l'on pourrait traduire non littéralement mais plus précisément par « fouille-merde ». Ils travaillent étroitement avec les lanceurs d'alerte.
[554] Entretien avec l'auteur, 08/04/2022.
[555] *Idem*.
[556] Entretien avec l'auteur, 30/03/2023.

***Boussole de disposition mentale* :**

1- Posture et intentionnalité

2- Culture et intelligence

3- Patriotisme et souveraineté

4- Organisation et cohésion

***Boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité

6- Méthodes et outils

7- Intégration et synergie

8- Plasticité et agilité

En vue d'approfondir l'analyse, nous reprenons l'analogie de la boussole et essayons d'appréhender le cap général suivi par les protagonistes de cette affaire.

1- Le cadre législatif peut-il s'adapter à la nouvelle donne engendrée par l'espace numérique ? Les profils d'hacktivistes, du moins ceux œuvrant à la liberté de l'information, pourront-ils être considérés un jour comme des hackers blancs, même s'ils outrepassent parfois la loi ? L'exemple de l'Allemagne montre avec le Chaos Computer Club qu'il est possible d'offrir une tribune institutionalisée aux hackers, ce dont la France n'a pas encore été capable. En outre, parmi les forces de sécurité, beaucoup pointent les failles des autorités judiciaires. Face à elles et paradoxalement, ce sont les avocats qui, mieux formés à ces enjeux, peuvent « […] *démonter le travail des gendarmes. Les enquêteurs doivent donc faire beaucoup de pédagogie, vulgariser, justifier, prouver pour la justice*.[557] »

2- Une culture du numérique et surtout de la cybersécurité est nécessaire en France chez les élites publiques en général. Les hackers et surtout les hacktivistes, en dépit de la méfiance qu'ils suscitent, sont aux dires de plusieurs observateurs les mieux placés si l'on veut, d'abord, accroître le niveau général de cybersécurité, ensuite être en capacité de mieux appréhender la cybermenace et s'y préparer, voire cyberdissuader les États offensifs dans le domaine. **Précisément, Pierre Penalba affirme que même si les hackers éthiques ont une posture offensive tout à fait à propos, « *Toutefois, ils n'utilisent/maitrisent pas les techniques les plus poussées et de très haut niveau en hacking/pénétration.* ***Car justement, ils ne sont pas dans la cybercriminalité, qui vise la plus grande efficacité avec un travail acharné à élaborer des armes numériques, à percer les défenses pour des raisons lucratives ou politiques***. » Et d'avouer, comme Clément Domingo, que **les profils**

[557] Entretien avec Stéphane Tonelli, 28/06/2017.

**gris sont les meilleurs**[558]. Ce dernier ajoute : « *Les vrais hackers sont des autodidactes et n'ont pas de diplôme d'ingénieur en sécurité informatique.* ***Très peu parmi les meilleurs spécialistes du hacking travaillent en France du fait d'une mauvaise valorisation à tous les égards***.[559] »

3- L'affaire *Bluetouff* a permis de dégager des éléments d'information sur la problématique de la souveraineté numérique de la France. Notamment l'usage d'une application comme *Whatsapp* par des officiers de la DGSI. Parfois, ces choix sont contraints car exigés des élites politiques, plus ou moins directement. C'est le cas avec le logiciel (*Gotham*) de science et analyse de données de Palantir Technologies qui a été adopté en 2015 par cette même DGSI – et le groupe Airbus –, vraisemblablement sous la pression d'autorités nationales désemparées face aux attentats terroristes. Un choix particulièrement décrié qui a réalimenté le sempiternel mais jamais tranché débat sur le lobbyisme américain. Le logiciel souverain européen qui devait succéder à celui de Palantir, *Artemis*, se fait toujours attendre en 2023. Par ailleurs, il faut noter qu'Olivier Laurelli a été entendu en mars 2021 dans le cadre de la Mission d'information sur la souveraineté numérique nationale face précisément au président de Palantir France, l'ancien directeur d'Airbus Helicopter, Fabrice Brégier[560].

4- Il faut noter que l'ANSSI reste en retrait car le statut des OIV, très récent, n'était pas encore clair à l'époque (LBDSN 2013 qui impose leur sécurisation). L'agence sera dotée d'un droit règlementaire de contrôles techniques sur leur sécurité par la LPM de 2013. Or, l'affaire se déroule concomitamment. On note donc des carences organisationnelles moins visibles aujourd'hui. Par ailleurs, le manque de cohésion est plus général, et la prise en compte de tous les acteurs de l'espace numérique n'est pas un réflexe. Le problème de la France avance « Alice », c'est « *l'ingérence du système ou le "hors système". Plusieurs forces s'opposent. Pas facile de faire bouger les lignes. Il y a une certaine paranoïa. On ne veut pas prendre de risques*.[561] » Si l'affaire *Bluetouff* concerne une affaire pénale, le manque d'homogénéité des autorités est toutefois flagrant. On constate plusieurs signaux divergents émis par les différentes institutions dont se fait l'écho la presse spécialisée. Comme l'atteste Julien Legay, spécialiste du renseignement sur la cybermenace dans le privé :

[558] Entretien avec Pierre Penalba, 07/07/2023.
[559] Entretien avec Clément Domingo, 15/11/2021.
[560] Voir le compte rendu de cette audition : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/souvnum/l15souvnum2021048_compte-rendu#. C'est sur la demande de l'entreprise américaine à participer aux discussions que Fabrice Brégier a été entendu et s'est soumis à la contradiction portée par les journalistes spécialisés Olivier Laurelli donc, et Olivier Tesquet de *Numerama*.
[561] Entretien avec l'autrice, 01/03/2023.

« *Les USA ont changé clairement leur fusil d'épaule au bénéfice de l'offensif. Du moins dans l'éducation. La France a été plus frileuse. Beaucoup d'acteurs étatiques vont dans le privé* », citant son N+1 chez Capgemini, ancien officier DGSE. « *Mais officiellement,* [pour le] *hackback ou* [le] *hacking offensif ça sera la DGSE ou du militaire et c'est classifié. Il y a une méconnaissance de la part des institutions judiciaires dans le hacking et l'offensif. Donc on est frileux en France. "Est-ce qu'on interfère avec une opé en cours de la part de l'État ?"… Plein de gens pourrait faire de l'offensif, mais rien n'est cadré dans cet aspect de l'offensif.* […] *L'ANSSI est très frileuse et à cheval sur le juridique ; moins* [chez] *les anciens de la DGSE. L'ANSSI a plus d'influence sur les acteurs économiques, donc on reste dans cette logique de frilosité et de rapport strict au droit*.[562] »

5- Il est plutôt légitime de pointer ici l'inadaptation manifeste des autorités judiciaires aux questions cyber, « *le décalage entre le monde du cyberespace et le monde judiciaire* » comme le fait remarquer l'officier de gendarmerie Christophe Torrisi[563]. En 2015 comme aujourd'hui, nous l'avons vu, le constat reste quasi-identique : si bon nombre d'avocats se sont spécialisés, peu de juges en revanche maîtrisent les aspects techniques et pourtant désormais incontournables des affaires liées aux TIC. S'agissant de transversalité, tout suggère que les différents organes de l'État n'ont pas la même approche de l'affaire et du sujet, voire du prévenu lui-même (statut, fonction, antécédents, état d'esprit…).

6- Ce point rejoint le sujet de la culture numérique carencée des autorités judiciaires. Là où, en revanche, des communautés de pratiques d'ordre technique relient le hacker *Bluetouff* (outils numériques, usage régulier et maîtrise des TIC) avec les services de sécurité de l'État. Prenons cette anecdote non liée à l'affaire mais caractéristique : Thomas « mxrch » Hertzog, jeune hacker éthique français – recruté en Suisse par ailleurs – a codé un programme d'OSINT basé sur l'exploitation de l'API de l'écosystème Google. Fin 2022, ce script *Python* baptisé Ghunt et fonctionnant sur l'OS Linux est déposé et gracieusement offert par son auteur sur la plateforme GitHub. Aussitôt, Thomas Hertzog s'attire la sympathie de la communauté des OSINTers avides de nouveaux outils, tandis qu'un gendarme N-TECH niçois le contacte sur LinkedIn pour le féliciter. Nul doute que ce dernier a testé cet outil voire ambitionnait de faire appel à son savoir-faire pour le compte de la gendarmerie[564].

[562] Entretien avec l'auteur, 13/10/2021.
[563] Entretien avec l'auteur, 23/08/2017.
[564] Cet officier est le chef du groupe de la lutte contre le cybercrime de l'antenne de la PJGN de Nice. Le jeune hacker de 21 ans ne répondra pas à sa sollicitation (entretien avec Thomas Hertzog, 14/06/2021).
*Python* est un langage informatique très utilisé et l'un des plus faciles à appréhender. https://github.com/mxrch/GHunt

7- Ce point semble inopérant ici compte tenu du rapport de force que représente cette confrontation judiciaire. Toutefois, le témoignage de M[e] Iteanu notamment est éclairant quant au manque de coordination qui affecte les autorités judiciaires et policières, pour ne parler que de ces organes de l'État. Le statut précisément informel des hacktivistes pose évidemment un problème épineux à la Justice et aux services de police en général. Ici, ils ne se désolidarisent pas forcément du prévenu mais n'ont pas à interférer en tout état de cause dans une instruction judicaire. En conclusion de notre entrevue, Olivier Laurelli a déploré l'inculture de la classe politique française et de la Justice vis-à-vis du numérique, et notamment de la culture hacker. « *Par défaut, les hackers sont perçus comme une menace par les autorités*. »

8- Nous avons évoqué la difficulté des autorités étatiques à se remettre en cause et à concrètement favoriser une évolution de leurs structures. L'institution judicaire est bien entendu d'autant plus concernée mais ceci est lié aux représentations fixistes qu'on se fait du droit, puisque par définition elles sont censées incarner la légitimité de décisions au nom de valeurs et de coutumes ancrées. C'est probablement à ce niveau, dans le regard porté sur les hackers que le socle culturel peut être réorienté dans une perspective de plus grande agilité. En tant qu'administrations publiques, les autorités policières ou militaires sont également entravées, mais sont toutefois capables de remises en question et d'une certaine adaptation aux contextes.

## Caractéristiques-clés – synthèse et hypothèses

Quels enseignements tirer de ce cas à partir des caractéristiques-clés, et ce dernier répond-il à nos hypothèses de recherche ?

• L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)

• L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)

• L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

### Synthèse :

Dans le cas qui nous occupe, les rapports qu'entretiennent hackers et autorités passent à travers le prisme d'une affaire pénale. Il est donc difficile de se prononcer aisément sur ces

liens. Toutefois, nous avons pu identifier des éléments notables relatifs aux frictions qui ont émaillé le cours de l'instruction judiciaire : difficulté de communication, les parties ne parlant pas le même « langage ». Ce qui n'est pas si étonnant en soi dans le cadre judiciaire pour des justiciables souvent peu au fait des lois. Mais il s'agit ici de s'approprier un univers technique qui échappe largement aux connaissances des magistrats en règle générale. Les enseignements significatifs de cette analyse sont les suivants :

- Les tenants de cette affaire montrent les craintes traditionnelles de structures étatiques condamnant par défaut ce qui sort du cadre législatif ou des procédures administratives. Plusieurs témoignages concordent pour dire que les autorités judiciaires ne sont pas assez formées aux codes et usages de l'espace numérique, alors même que celui-ci devient partie intégrante de la plupart des affaires pénales. L'affaire révèle plus largement le manque d'homogénéité entre les différents organes de l'État, puisque les autorités policières ont pu appuyer l'idée d'un acharnement exercé à l'encontre d'un activiste non dangereux. Olivier Laurelli a probablement servi d'exemple alors que d'autres menaces, de plus haut niveau celles-ci, se faisaient jour au début des années 2010 : le média Wikileaks notamment a suscité de grandes craintes chez les États occidentaux dont la France[565]. Le sort réservé à son fondateur, Julian Assange, en témoigne ouvertement. Plusieurs observateurs extérieurs ou défenseurs des libertés civiques affirment qu'on l'a brisé car soumis à des formes de torture psychologique.

- Nous avons évoqué les communautés de pratiques pouvant rapprocher les forces de sécurité et les hackers, en particulier sur le plan des outils numériques utilisés dans le cadre d'enquêtes par exemple. La question de l'OSINT et des techniques de recherche avancée sur les moteurs est en filigrane de l'affaire, puisque c'est par une sorte d'effet de levier réticulaire due à la sérendipité caractéristique des recherches sur le Web que tout a débuté. Le témoignage de Julien Métayer est intéressant : ayant atteint une grande notoriété via LinkedIn, notamment avec sa plateforme d'apprentissage de l'OSINT, celui-ci confie que son projet, très cadré notamment du point de vue de l'éthique, rassure les autorités, qui se sont d'ailleurs rapprochées de lui pour plusieurs projets de collaboration[566]. Pour revenir à l'affaire, comme hacktiviste, Olivier Laurelli affirme flirter avec la limite légale : « *Je cherche des failles des fois, je les exploite quand je sais que c'est utile et étrangement pour Amesys* […] *j'en ai exploité plein, et*

[565] Entretien avec Fabrice Epelboin, 08/04/2022.

[566] Entretien avec l'auteur, 30/03/2022. Il dit être devenu une interface, « *sans doute le pilote d'un vivier pour la sélection et le recrutement*. » (propos recueillis dans un cadre informel en septembre 2023). Ces projets sont contractualisés et ont une dimension éducative et opérationnelle, mais nous les tairons à sa demande. Voir son site de formation à l'OSINT : https://ozint.eu/

*j'ai jamais été attaqué pour ça. Et pour la Syrie encore plus, c'est très largement documenté sur reflets, et là encore aucune plainte. Pareil pour la Russie avec la radio de Gazprom. J'ai été poursuivi pour le truc le plus idiot, alors que oui et je m'en cache pas, je* pwn. *Mes* pwns *servent sûrement les bons intérêts il faut croire, et un jour j'ai rippé… ou plus simplement, une proc avait un agenda (et sur ce coup j'ai des preuves).*[567] »

- La nature même de l'affaire permet de comprendre qu'il ne pourrait y avoir de rapports sains et féconds entre les autorités étatiques en général et des hackers *gris* tels que *Bluetouff*. Difficile de dire si l'évènement a été propice à une collaboration ultérieure par exemple avec la DGSI, même si des liens, probablement d'amitié, ont été tissés, mais dans un cadre non professionnel. Le nœud du problème relève vraisemblablement du niveau de confiance qu'il est admis d'attribuer à des hacktivistes qui, selon Fabrice Epelboin, « *veulent la mort du système politique actuel.* […] *Il y a une vraie dualité entre la classe politique et les activistes/hacktivistes.*[568] »

Une interrogation reste en suspens. Nous ne pouvons pas juger du niveau technique réel d'Olivier Laurelli. Si, par mégarde de surcroît, il a été appréhendé très facilement par les autorités parce que son VPN le reliait directement à son identité numérique assez transparente, pourquoi avoir pris le risque de masquer très superficiellement celle-ci pour des recherches portant sur les sites gouvernementaux syriens ? Le régime Assad était alors sous le coup d'offensives informatiques par des hacktivistes, la *Syrian Electronic Army* (SEA)[569] devait donc veiller au grain et surveiller tous les accès légitimes ou illégitimes sur les sites gouvernementaux. Pourquoi dès lors ne pas avoir pris des mesures de sécurité opérationnelle (OPSEC) plus avancées ?

### Rappel des hypothèses :

1 – ces trois mondes (hackers–État–entreprises) sont intégrés et dans une co-construction (interaction et communication décloisonnées, projets communs, logique de dispositifs intelligents, synergie…)

[567] Entretien avec l'auteur, 30/03/2023. « Pwn » est un terme jargonneux du hacking signifiant « compromettre ».
[568] Entretien avec l'auteur, 08/04/2022.
[569] https://web.archive.org/web/20150606083305/http://sea.sy/index/en. L'OPSEC est un ensemble de mesures technico-logiques prises pour s'assurer de la meilleure confidentialité dans l'espace numérique.

2 – ces trois mondes sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas (incommunication) par manque de synergie

3 – ces trois mondes s'ignorent (acommunication)

Eu égard à tous les éléments dont nous disposons sur ce cas, nous pouvons considérer que malgré certains contacts très informels, il n'y a guère de rapports construits ou de synergie entre les acteurs. L'affaire remonte certes à 2015 au plus tard, mais elle reste caractéristique des difficultés de communication entre hackers – notamment hacktivistes – et autorités en particulier judiciaires dans le cas présent. Si l'on prend l'image du « dialogue de sourds » entre les intentions véritables d'Olivier Laurelli et la compréhension du sujet par les autorités judiciaires, nous pouvons privilégier la validation de l'hypothèse n°2.

* * *

### Résumé de l'étude de cas :

Le cas *Bluetouff* **nous a permis de comprendre que les codes des hackers sont difficiles à appréhender pour les institutions judiciaires**. Mis à part les avocats spécialisés contraints de s'y pencher ou par appétence pour le domaine, le fonctionnement des seules technologies numériques est étranger à la plupart des magistrats. Que dire dès lors d'une éthique hacker régie par la *do-ocratie* et selon laquelle la capacité d'action et de faire est érigée en principe philosophique fondamental ? **Cet état de fait engendre des situations où la communication entre des acteurs aux référentiels très différents est rendue difficile**. Enfin, le cas étudié donne cependant à observer que les services de sécurité (SR, police, gendarmerie) partagent des méthodes et des outils de travail (TIC/informatique) voire une certaine accointance d'esprit avec les hackers. Nous en sommes donc venu à valider l'hypothèse médiane numéro 2.

**Figure 38 :** *Tableau récapitulatif de l'étude de cas n°1*

| ***Boussole de disposition mentale*** | **Bilan – (Justice) ; Bilan ± (forces de sécurité/avocats)** |
|---|---|
| 1- Posture et intentionnalité | • Référentiels différents entre hackers et autorités judiciaires, rares magistrats spécialisés<br>• Connaissance des TIC chez les avocats spécialisés, eux très nombreux |
| 2- Culture et intelligence | • Culture du numérique et *a fortiori* de la sécurité informatique défaillante chez les magistrats<br>• Les hacktivistes sont considérés comme les meilleurs de leurs coreligionnaires (par rapport aux hackers *blancs*) mais sortent souvent du cadre légal |
| 3- Patriotisme et souveraineté | • Défaut de souveraineté et de « patriotisme numériques »<br>• Utilisation d'outils étrangers, dépendance technologique des forces de sécurité françaises |
| 4- Organisation et cohésion | • Amélioration du schéma organisationnel de sécurité depuis l'affaire<br>• Mais manque de cohésion générale et signaux divergents émis par les différentes institutions |
| ***Boussole du dispositif opérationnel*** | **Bilan – (Justice) ; Bilan ± (forces de sécurité)** |
| 5- Adaptabilité et transversalité | • Inadaptation et décalage du monde judiciaire<br>• Pas de vision commune avec les autorités de sécurité |
| 6- Méthodes et outils | • Méconnaissance manifeste des TIC chez les magistrats<br>• Communauté de pratiques entre hacktivistes et forces de sécurité |
| 7- Intégration et synergie | • Absence de coordination entre autorités sécuritaires et judiciaires quant au regard porté sur un hacktiviste comme *Bluetouff*<br>• *A priori* négatif vis-à-vis des profils hacktivistes |
| 8- Plasticité et agilité | • Point de vue des magistrats figé sur le droit<br>• Difficulté voire impossibilité à sortir de ce cadre rigide |

### 2) Les Élus et la culture hacker : le monde méconnu et incompris du hacking chez la classe politique

« *L'État, au mieux, vis-à-vis du numérique, est un singe inculte maniant une AK-47.* »

Fabrice Epelboin

En 2015 est publiée la *Stratégie nationale de sécurité du numérique* en vue d'opérer un *aggiornamento* numérique de l'État et des structures socioéconomiques du pays ; *la loi pour une République numérique* (LPRN) promulguée l'année suivante en est l'une des composantes et jalons essentiels. L'enjeu est de libéraliser l'accessibilité et la circulation des données ; protéger l'environnement numérique en général, donner un cadre légal au « hacking éthique » en particulier. La LPRN d'octobre 2016 est adoptée dans le cadre du plan d'action global de la « stratégique numérique » intitulé *La République numérique en actes*. Cette loi est venue indirectement consacrer le statut de « hacker éthique », à savoir nous l'avons vu des experts en sécurité informatique autorisés à utiliser des techniques offensives d'intrusion dans le cadre de missions contractuelles auprès d'organisations publiques ou privées. Plus tard, dans le mouvement général post-Covid de réflexion sur la réindustrialisation et la réhabilitation de la notion de souveraineté nationale, les Parlementaires ont décidé de questionner celle de souveraineté numérique. Ces débats ont donné lieu à la tenue de plusieurs missions d'informations ou commissions d'enquête visant à éclairer la position de la France et de mieux comprendre la plus-value des hackers quant à la cybersécurité nationale.

Pour autant, si elle accorde une place aux *chapeaux blancs*, la LPRN fait encore preuve de timidité et évoque le statut de *lanceur d'alerte de sécurité* plutôt que de mentionner nommément les « hackers ». Un positionnement ambigu qui va possiblement être clarifié avec un amendement à la loi daté de juin 2023, sept ans tout de même après la publication du texte original.

#### a) *Un dilemme cornélien pour l'État français*

C'est en 1988 que la loi Godfrain autorise la répression des actes de piratage informatique dont la traduction dans le Code pénal se prolonge en 2004 puis 2013 dans les article 323-1 (accès et maintien frauduleux STAD) et 323-3-1 (divulgation de vulnérabilités)[570]. Ces articles avaient été particulièrement critiqués comme en attestent les propos d'Éric Filiol : « *Je n'ai*

[570] L'on pourra se faire une idée claire des tenants et aboutissants de ces dispositions légales dans l'analyse de Fabrice Mattatia, « Faut-il dépénaliser les hackers blancs ? », *Revue de science criminelle et de droit pénal comparé*, 2015/4 (N°4), pp. 837-846. Pour une approche critique de la loi Godfrain, voir https://web.archive.org/web/20160418055109/https://www.hackersrepublic.org/cultureduhacking/la-loi-godfrain-explications-et-illustrations

*jamais vu autant de rejets face à un article de loi* […] *qui n'est plus du tout adapté et qui finalement met dans le même sac les pirates et les hackers. Et cela, c'est la pire erreur à faire. On est dans une situation ubuesque : rien n'interdit à un individu de dénoncer le fait qu'une voiture soit vendue sans frein, dans le monde logiciel, l'individu serait condamné*.[571] » Cette approche juridique renvoie bien évidemment à l'affaire « Bluetouff » que nous avons traitée plus avant, laquelle est d'ailleurs mentionnée par les parlementaires, certains reconnaissant à propos d'Olivier Laurelli « […] *qu'il n'avait entrepris aucune démarche offensive* […]. *Ce qu'il avait fait n'était pas en soi répréhensible*.[572] »

La préparation de la LPRN de 2016 sous la forme du rapport de commission (janvier) pour le projet de loi n°3318 est illustrative des discussions qui ont occupé les parlementaires[573]. « *Il est toujours compliqué de donner le statut de lanceur d'alerte à des hackers*. » avise l'un des rapporteurs. Comme le souligne *a posteriori* Guillaume Poupard, « *Le terme "lanceur d'alerte" pour désigner les hackers, ça parlait aux parlementaires, ça montre la méconnaissance. Et tous les textes sur le numérique, c'est pareil. Les parlementaires n'ont pas la culture numérique*.[574] » Des propos croisant ceux de Jean-Marc Manach pour qui, « *du côté de la classe politique, il y a un vrai problème de culture et de connaissance en termes de cyberespace, au Parlement par exemple. Les rares qui maitrisaient le sujet ont été balayés*.[575] » Selon Guillaume Poupard du reste, seule Axelle Lemaire, ancienne Secrétaire d'État chargée du Numérique et de l'Innovation sous François Hollande, « *comprenait un peu les enjeux du numérique, mais pas vraiment ceux de la sécurité du numérique. Il ne fallait pas mélanger les deux.* » Or, la clause du texte fait l'objet d'un amendement proposé à l'époque par Nathalie Kosciusko-Morizet afin de clarifier le statut de *lanceur d'alerte de sécurité*, alors même que celui de lanceur d'alerte classique n'était toujours pas fixé avec précision, comme le laissent entendre les mots de la députée Isabelle Attard : « *Je regrette que le projet de loi relatif à la protection du secret des sources des journalistes ait été reporté et que nous ayons restreint la catégorie des lanceurs d'alerte à quelques professions – je ne sais pas ce que nous aurions fait si l'affaire Snowden s'était produite dans notre pays*.[576] » À ce stade, la commission rejette l'amendement car les députés ne parviennent pas à s'accorder sur les suites pénales à appliquer, les *lanceurs d'alerte de sécurité* disposant *a priori* d'exemptions de peine, ce qui générait des craintes chez plusieurs parlementaires.

[571] https://www.lemonde.fr/blog/bugbrother/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/
[572] https://www.assemblee-nationale.fr/14/rapports/r3399.asp
[573] *Ibidem.*
[574] Entretien avec l'auteur, 17/04/2023.
[575] Entretien avec l'auteur, 10/04/2023.
[576] https://www.assemblee-nationale.fr/14/rapports/r3399.asp

En octobre 2016, la LPRN consacre finalement le statut de *lanceur d'alerte numérique* sans réellement parvenir à caractériser ce que sont les hackers légaux. Néanmoins, c'est une avancée dont se réjouissent les principaux concernés. Ainsi, selon l'article L2321-4 du Code de la défense :

> « *Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.*
> *L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa au présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information*.[577] »

L'on comprend dès lors l'intérêt de voir évoluer la loi pour permettre aux hackers éthiques de venir suppléer voire éclairer le travail des RSSI qui ont une vision trop internalisée quant à l'intégrité supposée de leur SI. Par ailleurs, la loi Godfrain était toujours effective lorsqu'une personne de bonne foi remontait l'information et qu'il ne trouvait aucun canal sécurisé (via chiffrement) auprès d'une autorité vers laquelle communiquer les informations (rapports de vulnérabilités) sur les failles de telle ou telle entité. La LPRN vient combler ce vide en assignant à l'ANSSI le rôle d'interlocuteur dans les meilleures conditions de sécurisation et ainsi éviter les remontées « sauvages ». Cette centralisation de l'identification se fait également par le biais des plateformes spécialisées (YesWeHack, Yogosha en France) qui mettent en place des mécanismes de divulgation de vulnérabilités (*Vulnerability Disclosure Program* – VDP) pour mieux encadrer et identifier les hackers effectuant ces signalements. Par ailleurs, l'Union européenne va renforcer sa directive NIS1 par une deuxième version (NIS2)[578] qui sera mise en vigueur en France au second semestre 2024. NIS1 impose aux acteurs de dix secteurs-clés de déclarer leurs incidents de sécurité. Parmi les dispositions de NIS2, on notera la possibilité accordée aux hackers de préserver leur anonymat dans le cadre d'une remontée de vulnérabilité auprès d'un CSIRT national (*Computer Security Incident Response Team*)[579]. Si ces progrès sont encourageants, il aura fallu sept ans pour envisager, de surcroît à l'initiative

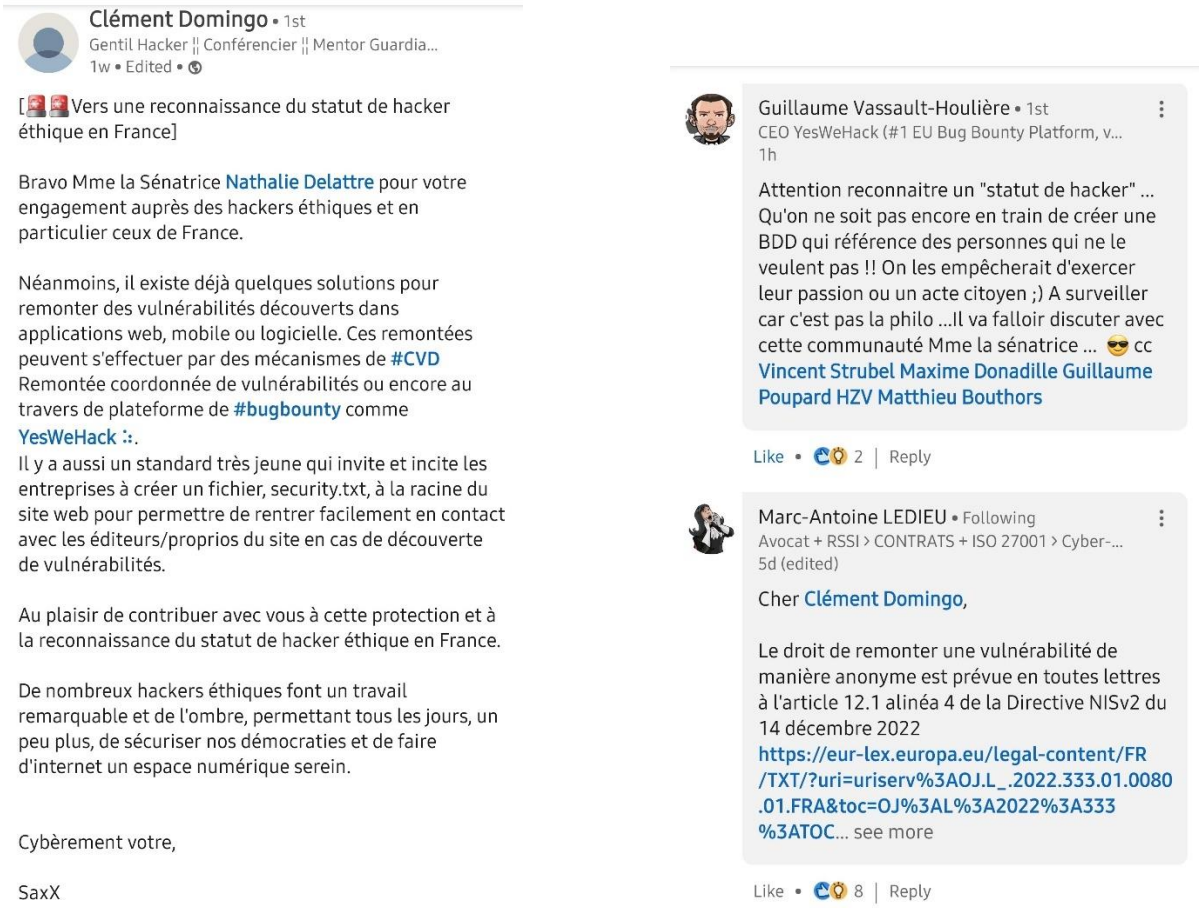
[577] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203174
[578] *Network and Information Security*. https://www.ssi.gouv.fr/directive-nis-2/. NIS2 encourage notamment les entreprises et acteurs publics à faire remonter leurs vulnérabilités critiques à l'ENISA, l'agence européenne pour la sécurité des réseaux et de l'information (https://www.enisa.europa.eu/).
[579] Pour la France, c'est le CERT-FR de l'ANSSI (https://www.ssi.gouv.fr/agence/organisation/les-sous-directeurs/centre-operationnel-de-la-securite-des-systemes-dinformation/le-cert-fr/). CSIRT et CERT sont équivalents, mais ce dernier acronyme est une marque américaine (*Computer Emergency Response Team*). Voir https://www.cyber-securite.fr/un-csirt-a-quoi-ca-cert/. Voir l'article 12-1-4 de la directive NIS2 : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555.

individuelle d'une sénatrice, Nathalie Delattre, de renforcer la protection des hackers éthiques, dont le statut demeure toujours assez flou[580]. Guillaume Poupard signale que « *La nécessité d'anonymiser ou pas les remontées de failles est très discutée. La loi dit que l'ANSSI n'est pas obligée de dénoncer de telles alertes. Mais le niveau d'équilibre en France n'est pas trop protecteur pour les gens honnêtes. La loi pour la République numérique de 2016 ne légalise pas formellement le hacking éthique*.[581] »

### b) *Des avancées juridiques mais une classe politique encore peu éclairée*

L'initiative de Nathalie Delattre vise à amender la disposition de la LPRN en vue d'entériner la reconnaissance du statut de hacker éthique en droit français, au-delà de celui de lanceur d'alerte traditionnel dans lequel il a été inséré avec une certaine maladresse. En effet, la LRPN n'autorise pas les hackers à contacter directement les éditeurs de logiciels concernés par une faille mais contraint à passer par l'intermédiaire de l'ANSSI ; ce qui pourrait possiblement engendrer, d'une part, des retards dans la prise en charge de ces vulnérabilités, d'autre part des poursuites légales engagées par certains éditeurs mettant en doute la bonne foi des lanceurs d'alerte numérique. Il est intéressant de noter que plusieurs hackers ont accueilli cette proposition d'amendement avec les honneurs, à l'image du commentaire de Clément Domingo sur LinkedIn. Par ailleurs, l'on peut observer les encouragements dubitatifs ici de la part du PDG de la plateforme de *bug bounty* YesWehack, Guillaume Vassault-Houlière, appelant la sénatrice à consulter directement les hackers et conviant plusieurs figures-clés de la haute administration à participer à cette réflexion[582].

[580] https://www.senat.fr/seances/s202306/s20230628/s20230628008.html
[581] Entretien avec l'auteur, 17/04/2023.
[582] Notamment, Vincent Strubel et Guillaume Poupard, respectivement actuel et ancien directeurs de l'ANSSI ; Maxime Donadille, conseiller TIC et cybersécurité à Bercy ; HZV (Hackerzvoice), l'association qui organise l'évènement *Le Hack* (https://hzv.fr/).




*Posts LinkedIn réagissant à la proposition d'un amendement d'appel émise par la sénatrice Nathalie Delattre, juin 2023.*

La proposition de Mme Delattre représente une avancée significative dont on verra si elle aboutit. Elle tend timidement vers la législation particulièrement novatrice de la Belgique qui a récemment généré la stupeur chez bon nombre de pays européens, dont la France, en autorisant les hackers éthiques à tester les sécurités d'une organisation sans en demander l'autorisation, et à pratiquer – sous conditions préalables – la divulgation publique des vulnérabilités[583]. Cette *Loi sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé* constitue une sorte de reconnaissance à 360° du droit de divulgation de vulnérabilités. Comme l'indiquent deux juristes de Yogosha, « *Parmi les États membres, la Belgique se démarque en offrant le cadre juridique le plus avancé pour protéger les hackers éthiques, devançant ainsi les autres pays dans ce domaine*.[584] » Pour une hacktiviste comme « Alice »,

[583] https://www.ejustice.just.fgov.be/eli/loi/2022/11/28/2022042980/justel#LNK0013. Promulguée en novembre et publiée en décembre 2022, puis entrée en vigueur en février 2023.
[584] https://www.village-justice.com/articles/hacker-ethique-detecter-les-vulnerabilites-pour-prevenir-les-cyberattaques,46474.html

« *la nouvelle loi sur le hacking en Belgique est une accélération de la cyberguerre. C'est une sorte de filets lancés aux gros poissons : il y a derrière cette posture une espèce de logique de recrutement des "bons".* » La presse belge vient appuyer indirectement ces propos, en expliquant que le but est de « *profiter de l'expertise de cette communauté, toujours plus nombreuse, en matière de détection des failles informatiques. Un cadre juridique unique en Europe qui pourrait donc venir renforcer les performances en matière de Cybersécurité de la Belgique, déjà plutôt bonne élève en la matière.*[585] » Et « Alice » de poursuivre : « *La Loi pour la République numérique de 2016 montre que les institutions ne te protègent pas si tu ne te protèges pas toi-même. Cette loi montre qu'il y a des précautions énormes à prendre, juridiques notamment… Et c'est aussi comme une phase de recrutement pour les entreprises.*[586] »

Pourtant, les élus français s'inquiètent du positionnement belge dont ils pensent qu'il ouvre une boîte de Pandore. Pour Guillaume Poupard, « *Le débat en Belgique, et la nouvelle loi sur l'évaluation libre des failles de sécurité, font peur en France. On redoute l'effet d'aubaine que ça peut générer, et qui bénéficierait aux criminels. De plus, les éditeurs n'aiment pas le* full disclosure*, donc d'autres pays vont plus loin. On pense que plus on va protéger les hackers, plus on va avoir un effet d'aubaine. L'équilibre pourra peut-être évoluer en France. Il faut au moins éviter les erreurs judiciaires.*[587] » Une opinion mi-obligée, mi-critique donc, pour cet ancien serviteur de l'État néanmoins pragmatique quant à la nécessaire adaptation du pays vis-à-vis des questions cyber. Si le regard des autorités a un peu changé vis-à-vis des hackers éthiques avec la LPRN comme le concèdent Alexandre Oda ou Fabrice Epelboin, qui parle surtout de « *l'influence de la culture pop/geek (Bureau des légendes, Mr Robot), la vision amalgamant criminalité et hacking a longtemps prévalu en France*. » Ainsi, plusieurs observateurs ou hackers mentionnent invariablement les exemples américain et allemand ou encore israélien. Du côté de ce dernier pays, fondateur de la plateforme d'OSINT *Epieos*, Sylvain Hajri parle d'une émulation puissante de l'unité spécialisée 8.200 de Tsahal qui engendre des entreprises privées « *qui ne sont pas forcément toutes sulfureuses et même ont pignon sur rue et jouissent d'une excellente réputation.* […] *En France, il y a une créativité qui est entravée dans ces domaines.*[588] » Alexandre Papaemmanuel souligne, quant à lui : « *Les États-Unis font rayonner leur approche, leurs mots à eux, leurs notions/concepts. C'est une guerre des concepts autour des technologies, dont le cyber. Or, qu'est-ce qu'apporte la France là-dedans ? Dans le GEOINT, c'est OK, voire au-delà de ce qui suffirait. Mais pas dans*

[585] https://www.rtbf.be/article/inedit-en-europe-la-belgique-instaure-une-protection-pour-les-hackers-ethiques-sous-certaines-conditions-11156779
[586] Entretien avec l'autrice, 01/03/2023.
[587] Entretien avec l'auteur, 17/04/2023.
[588] Entretien avec l'auteur, 27/02/2023. (https://epieos.com/).

*le numérique*.[589] » Pour « Alice », « *la législation française est punitive, la législation américaine est négociatrice : avantage/faiblesse, rapport coût/bénéfice typique d'une culture capitaliste forte*.[590] » Outre-Rhin, le Chaos Computer Club tient, on l'a dit, une place prépondérante et constitue une véritable institution et un cercle de dialogue avec l'État, en agissant comme un contre-pouvoir sur les questions liées à la protection de la vie privée, la sécurité informatique ou la démocratie. D'après le député européen Jan Philipp Albrecht, « *le CCC a grandement contribué à la tenue d'un débat éclairé sur la cybersécurité et la gouvernance de l'Internet en Allemagne*.[591] » Le cas du CCC est très intéressant et fera l'objet d'une attention particulière dans les lignes qui suivent.

### c) *Clé de lecture du cas d'étude*

Cette étude partielle et longitudinale du regard posé par la classe politique sur les hackers soulève plusieurs interrogations. Prenons cet extrait significatif de discussions parlementaires rapportées sous la forme d'un compte rendu sur un projet de loi d'orientation et de programmation du ministère de l'Intérieur à la fin 2022 :

> « ***M. Jean-François Coulomme :***
> *Nous avons longuement évoqué, dans le cadre de nos échanges relatifs à la cybercriminalité, les atteintes commises contre des intérêts commerciaux ou contre des administrations – chacun a par exemple constaté que des hôpitaux ont récemment été touchés par des actes de cybercriminalité. L'amendement vise à prendre également en considération les utilisateurs particuliers, eux aussi victimes de ces agressions numériques qui peuvent prendre des formes multiples – phishing, ou hameçonnage, perte de données, blocage d'ordinateur, cryptage de disque dur, etc.*
> *Nous estimons qu'il est de la responsabilité de l'État de définir un code de bonne conduite, ou au moins de mettre à disposition des outils de formation pour permettre aux citoyens de se prémunir de ce type de dommages informatiques.*
> ***Mme Anne Le Hénanff :***
> *Ça existe déjà !*
> ***M. Jean-François Coulomme :***
> *Probablement, mais un guide de bonne conduite qui serait élaboré par des professionnels du hacking et autres spécialistes de l'informatique pourrait être mis à disposition sur les*

[589] Entretien avec l'auteur, 26/07/2017. Le GEOINT est le renseignement d'origine géospatiale (produit à partir des images aériennes et satellitaires).
[590] Entretien avec l'autrice, 01/03/2023.
[591] http://owni.fr/2011/11/03/30-ans-de-bidouille/index.html

*plateformes gouvernementales, par exemple sur le site impots.gouv.fr. (Applaudissements sur les bancs du groupe LFI-NUPES).*[592] »

Indépendamment de toute considération partisane, ces échanges sont à l'image du bilan que l'on peut dresser de cette étude : d'abord, on note une certaine prise de conscience du risque cyber ; ensuite, on remarque le degré d'amateurisme des élus s'agissant des questions de sécurité informatique. Nous pensons que c'est révélateur du fait que par la force des choses la cybersécurité s'invite à l'agenda politique, mais que nous sommes très éloignés d'un dialogue ouvert entre les élus et ce qui pourrait constituer un vrai CCC français.

- ***Disposition mentale – 1ère caractéristique : la complexité du réel et du « village global »***

On l'a vu, si les initiatives et prises de conscience individuelles existent bel et bien en France, on assiste souvent à un manque flagrant de culture numérique et cyber. L'exemple positif d'Isabelle Attard est intéressant, qui prêche la bonne parole, possiblement dans le désert néanmoins : « *Tous ici, nous pouvons nous comporter comme des lanceurs d'alerte pour tester la véracité des conditions d'utilisation d'une plateforme, en y mettant de fausses informations. Nous pouvons ainsi vérifier, comme le font les journalistes, si nos données sont bien protégées. J'espère que nous sommes nombreux à le faire, ce qui nous permettra d'avoir de vrais débats en séance et de résoudre rapidement ce problème.*[593] » Malheureusement, la plupart des élus ne pensent pas de la sorte, en attestent les multiples exemples cités par Jean-François Loewenthal notamment ou Florent Curtet. Le premier nous fait part de l'anecdote suivante : un député d'En Marche, qui pourtant évolue dans le lobbying et les TIC, lui commande une étude de *due diligence* sur sa personne. « *Il ne semble pas très expert*, dit Jean-François Loewenthal, *car ne maîtrise pas sa e-réputation, son identité numérique : CV un peu retouché, etc.*[594] » Pour sa part, Florent Curtet livre plusieurs anecdotes significatives sur cette même inculture de la sécurité numérique des élus pourtant hauts placés, citant l'exemple de députés utilisant un mot de passe identique sur plusieurs services en ligne et leurs activités professionnelles[595]. La conscience des enjeux de sécurité des élus semble par

[592] https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/seance/session-ordinaire-de-2022-2023/troisieme-seance-du-jeudi-17-novembre-2022
[593] https://www.assemblee-nationale.fr/14/rapports/r3399.asp
[594] Entretien avec l'auteur, 26/06/2017. La *due diligence* ou « obligation de vigilance » en droit français, est une forme d'investigation sur l'état financier d'une entreprise ou futur partenaire dont on veut vérifier la solvabilité. Ici, le concept est utilisé par déformation pour désigner une enquête sur l'image et la réputation d'une personne.
[595] Florent Curtet, *Hacke-moi…*, *op. cit.*, pp. 180-181.

conséquent très faible, comme en témoigne Éric Filiol, bien placé pour juger du système politique :

> « *D'abord, il faut savoir que, en France en tous cas, la formation des hommes politiques est inadaptée à l'évolution du monde technologique. Nous avons des gens qui ont fait souvent ce qu'on appelle leurs humanités, c'est à dire, c'est une formation plus droit, histoire du droit éventuellement, pour les moins littéraires économie, mais on se retrouve en situation où nous avons des décideurs qui ne comprennent plus rien à la technologie et qui prennent des décisions, malheureusement, qui impactent nos vies. Il faut savoir que l'informatique, les technologies de l'information et la sécurité qui va avec, maintenant concernent nos vies, quand on va à l'hôpital, quand on déclare nos impôts, bref, dans les moindres faits et gestes. Ça c'est important de le savoir. Donc nous avons des hommes politiques qui ne comprennent plus la technologie. Si tant est qu'ils ne l'aient jamais comprise un jour. Alors, ce n'est pas gênant dans l'absolu, parce qu'on ne peut pas être spécialiste en tout. Ça veut dire que comme c'est le cas dans certains pays, je pense en particulier à l'Allemagne qui a su, effectivement, capitaliser sur sa communauté de hackers. Ça veut dire qu'il faut être bien entouré. Il faut avoir des conseillers qui, effectivement, ont un sens de l'État. Et je pense que depuis le Général de Gaulle ce sens s'est beaucoup perdu.*[596] »

Un constat partagé par Fabrice Epelboin, pour qui « *En France, soit on attaque juridiquement l'État pour des lois "débiles", il y a plus de confrontation ; soit on ridiculise les hommes politiques car ils n'y connaissent rien.* » Et de mentionner l'épisode de Cédric O, ex-secrétaire d'État au numérique, tentant de montrer à l'assemblée que l'utilisation d'un VPN rendait inutile l'interdiction de l'anonymat en ligne, sous couvert de présenter aux députés ce qu'est ce dispositif de confidentialité, pour ce qui s'est apparenté aux yeux de beaucoup de spécialistes à une véritable opération de *sponsoring* publicitaire, même discrète, pour *NordVPN*[597]. Enfin, selon Fabrice Epelboin, seuls quatre ou cinq députés connaissent un minimum les questions numériques.

[596] Interview d'Éric Filiol sur la chaine *Thinkerview*, *op. cit*.

[597] Entretien avec l'auteur, 08/04/2022. Voir https://www.youtube.com/watch?v=TlX0lYRQB3A. Ce qui pourrait sembler partir d'une bonne intention montre en réalité la méconnaissance de l'ex-secrétaire d'État, puisqu'en réalité un VPN ne permet pas l'anonymat mais assure seulement une certaine confidentialité et le respect de la vie privée en condition normale d'usage, ce qui n'est pas la même chose. D'ailleurs, en 2021, sur la base d'une simple injonction judiciaire visant non des profils dangereux mais des activistes de Youth for Climate militant pour le droit au logement, la police française a fait pression sur la Suisse pour qu'elle-même enjoigne à l'entreprise nationale Proton Technologies AG d'identifier et livrer les activistes en question. Pour plus détails sur l'affaire, voir https://www.numerama.com/tech/736940-protonmail-transmet-des-adresses-ip-a-la-police-4-questions-pour-comprendre-la-polemique.html.

- ***Disposition mentale – 2e caractéristique : culture de l'intelligence rusée***

Si l'on ne comprend pas bien le contexte dans lequel on évolue, il est évident qu'on ne puisse s'y mouvoir habilement. Comme le dit le LCL Leberon : « *Le cyber est le vecteur, mais la culture cyber, on ne l'a pas forcément en France. On y vient pour le renseignement*.[598] » À l'image de ces propos, la culture nationale joue un rôle important dans la manière de voir les choses. Clément Domingo va jusqu'à dire que l'organisation du travail en France peut avoir un impact à cet égard, quand il évoque une culture du travail décalé encore faible là où les pays anglosaxons ou l'Allemagne l'ont bien plus développée. Pour lui, cela constitue un frein indirect à l'ouverture d'esprit, évoquant l'administration française notamment mais aussi une partie des entreprises, sauf sociétés spécialisées, spécifiques, qui ont su adapter leur organisation[599].

Comment appréhender le cyber, milieu par excellence où se déploie la ruse et se joue une compétition globale ? Comme le note Guillaume Poupard au sujet de l'adaptation que l'administration doit opérer et le regard erroné qu'elle porte aux hackers : « *Il y a donc un gros travail de pédagogie à faire auprès des élites politiques. Au bilan, on préfère que ce soit globalement interdit* [l'activité de remontées de failles]*, sauf avec des gens honnêtes. C'est l'équilibre auquel on est arrivé en France. Avec une Justice qui est très frileuse pour changer des choses dans la loi*.[600] » La question qui sous-tend ce constat est la suivante : nos dirigeants pensent-ils que les hackers sont tous invariablement malhonnêtes ? Le point de vue de Fabrice Epelboin est sévère : « *La Loi pour une République numérique de 2016 n'en est pas vraiment une, mais une correction de dispositions idiotes préalables*.[601] »

En définitive, en écho à un point de la première partie de notre travail portant sur les relations entre ruse et cyber, les propos de Jean-Vincent Holeindre montrent toute leur pertinence :

> « *Nous éprouvons aujourd'hui de la difficulté à nommer "guerres" ces conflits de ruse* [...] *À vrai dire, nous ne sommes pas sortis — particulièrement en France où l'imaginaire aristocratique et chevaleresque demeure puissant — de cette arrogance de la force et de ce mépris de la ruse* [...]. *Machiavel dit bien que c'est la ruse qui transforme la force en puissance. La force ne constitue pas en tant que telle une puissance. Or, la ruse est peut-être ce qui manque aujourd'hui aux stratégies contemporaines. Non pas au sens tactique, qui est pleinement maîtrisé par les armées, mais au sens stratégique, et donc politique, de la mètis grecque, fondée sur l'anticipation et l'adaptation.* [...] *ce faisant, nous ne voulons pas véritablement nous résoudre à penser et à faire la guerre autrement.* [...] *Les puissances occidentales ont beaucoup de difficulté à anticiper, à voir*

[598] Entretien avec l'auteur, 21/06/2017.
[599] Entretien avec l'auteur, 15/11/2021.
[600] Entretien avec l'auteur, 17/04/2023.
[601] Entretien avec l'auteur, 08/04/2022.

*loin, et à s'adapter, c'est-à-dire à sortir d'un certain confort intellectuel pour penser hors du cadre établi.*[602] »

- ***Disposition mentale – 3e caractéristique : le triptyque patriotisme–unité–souveraineté***

C'est un fait, les missions d'information ou commissions organisées à l'initiative de certains parlementaires et sénateurs, souvent de manière transpartisane, sont encourageantes. En particulier, les interrogations sur le degré de souveraineté numérique du pays sont fort louables. Mais ces rapports sont-ils suivis d'effets et de faits ? Ainsi que le note Victor Poucheret, « *C'est évidemment insuffisant*.[603] » À en croire Fabrice Epelboin, il faudra ni plus ni moins attendre de changer de génération pour que les politiques puissent probablement prendre leur mesure et mieux saisir les enjeux de sécurité numérique. Pour lui, « *ça s'améliorera possiblement, si on en finit avec les lois portées par les lobbies et les conflits d'intérêts politiques*.[604] » Et d'évoquer l'ambivalence des élites quant aux hackers qu'on méprise mais dont on a besoin. « *La classe politique a commencé à avoir peur et se méfier du cyber par ignorance et quand les affaires Wikileaks ont commencé. Tant que ce système, cette culture politique en France continuera, on aura cette défiance.* » Selon lui, « *Il y a un aspect culturel puissant : celui d'une défiance et d'un mépris initiaux des autorités françaises à l'égard des hackers.* » Il parle d'un environnement longtemps resté hostile et toxique pour eux, poursuivant : « *Aujourd'hui, du moins, on est en transition avec une rémission de cette culture toxique. Mais c'est la classe politique qui pose problème : ignorante et méprisante, à cheval sur ses privilèges établis donc hostile par nature à une culture alternative telle que celle du hacking*.[605] »

Les questions de souveraineté et de patriotisme se posent par ailleurs avec les pratiques de lobbyisme auxquelles la France est confrontée, si tant est que les élites politiques en aient conscience ou en fassent grand cas. Le constat de Jean-Nicolas Piotrowski est sans appel pour qui le lobbying américain en général affaiblit la souveraineté nationale, rappelant l'affaire Palantir et son rapprochement avec Airbus et la DGSI. On peut noter en complément les stratégies de conquête agressives opérées par cette société spécialiste de l'analyse de données qui a visé opportunément les institutions hospitalières comme l'AP-HP (Assistance publique - Hôpitaux de Paris) durant la pandémie du Covid-19. Jean-Nicolas Piotrowski affirme que les militaires français, de leur côté, sont en partie tenus – « *financés* » – par l'influence

[602] Jean-Vincent Holeindre (dir.), « Les deux visages de la guerre », *op. cit.*, p. 388, et https://geopoweb.fr/?LA-RUSE-ET-LA-FORCE-AU-COEUR-DES-RELATIONS-INTERNATIONALES-CONTEMPORAINES.
[603] Entretien avec l'auteur, 14/11/2021.
[604] Entretien avec l'auteur, 08/04/2022.
[605] *Ibid.*, 08/04/2022.

américaine, et que l'Armée est vraisemblablement partagée entre souverainisme et inféodation aux États-Unis[606]. L'entrepreneur français persiste : le pays a loupé le coche, et développer des outils en interne pour les SR coûterait trop cher en R&D étant donné le retard accumulé. ITrust et des entreprises françaises similaires sont approchées par des fonds d'investissement américains ou encore des géants du secteur comme IBM ou CISCO. « *Il y a*, conclue-t-il, *un problème de stratégie industrielle d'une manière générale. Une rupture dans le cercle économique vertueux* [...], *les sociétés françaises qui ne peuvent pas exporter... Pas de stratégie, pas de commande publique*.[607] »

Au-delà de ces difficultés malheureusement habituelles, les acteurs du cyber ont bien du mal à s'entendre. D'aucuns déplorent des réflexes clientélistes éculés, comme Karim Lamouri qui n'est pas tendre avec l'initiative *Hack4values*, portée notamment par la plateforme Yogosha[608]. Selon ce dernier, « *entre les acteurs de terrain et l'État, les relations sont nulles. Ou alors, c'est du copinage et de la communication. Comme pour Hack4values : ils discutent avec Jean-Noël Barrot et les députés, mais ils font de la diplomatie, c'est du copinage*. » À propos de la souveraineté numérique et de la volonté de voir changer les autorités françaises, il s'entend souvent dire : *« Pourquoi tu te fais chier avec ça ? on admire ta volonté, mais reste où tu es*. » Karim Lamouri ironise : « *Si on attend des autorités qu'elles bougent, on est morts*. » Évoquant ce qu'il assimile à de l'immobilisme de la part de l'État, il ajoute : « *Selon la définition du fou par Einstein, on est des fous. On fait tous les jours la même chose. Et on ne change pas*. [...] *Ce que fait Nathalie Delattre, c'est bien. Proposer un OS français souverain, c'est bien, mais il faut s'occuper des bases : par exemple quand on utilise des clouds américains, ça ne sert plus à rien, idem pour les smartphones*.[609] »

Une appréciation de la situation qui n'est pas sans rappeler le constat de Sylvain Hajri, fondateur de la plateforme Epieos, au sujet des rapports autorités|hackers : « *il y a plein de bonnes volontés pour réunir les deux mondes, mais* [*c'est*] *le copinage qui gangrène ces interactions*. » Et d'évoquer comment il a pu, au sein de l'*OSINT village* qu'il organise dans le cadre de l'évènement *Le Hack*, inviter des fonctionnaires de police et des militaires qu'il n'aurait, sans ce biais-là, pas pu rencontrer. Ces invitations sont honorées et c'est ce qui lui permet de dire qu'il y a malgré tout une manifestation d'intérêt de la part des autorités, mais un intérêt encore « *complexé*. » Sylvain Hajri relate son projet avec Epieos et souligne avoir été ciblé par des intérêts adverses étrangers mais aussi français lorsque son entreprise prenait

[606] Entretien avec l'auteur, 03/07/2017. Il est le PDG de la société ITrust.
[607] *Ibid.*, 03/07/2017.
[608] https://hack4values.eu/
[609] Entretien avec l'auteur, 07/07/2023. Karim Lamouri est cofondateur de HWB. Jean-Noël Barrot est en 2023 ministre délégué auprès du ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, chargé du Numérique.

son envol. Il dit avoir détecté le montage d'une campagne de dénigrement à son encontre qui aurait été véhiculée par le médium bien connu des spécialistes du renseignement et de l'IE, *Intelligence Online*. Enfin, il s'interroge sur le paradoxe de disposer de clients étrangers (Anglosaxons en particulier) plutôt que français, et relate une anecdote sur son invitation au siège lyonnais d'Interpol en mars 2023. Ses hôtes sont en effet des policiers de nationalité australienne s'intéressant de près à sa plateforme[610].

- ***Dispositif opérationnel – 4e caractéristique : l'information au centre du jeu stratégique***

Parmi les organismes cherchant à s'entourer de hackers éthiques, on compte le COMCYBER au premier plan avec les DGSE et DGSI. Il recrute ainsi dans la communauté amateurs avec, selon Frédérick Douzet, un esprit, le *mindset* des hackers, ajoutant : « *Aux États-Unis, ça fait longtemps*.[611] » Ainsi, il essaie d'attirer les profils via des *hackatons* ou autres CTF. La culture française de la « fiche de poste » a commencé à s'atténuer grâce à l'ANSSI, du moins sous le mandat de Guillaume Poupard fait remarquer Fabrice Epelboin. Toutefois, plusieurs profils n'ont pas attendu ce virage trop tardivement opéré en France. Ce dernier cite notamment le cas de Matthieu Suiche, hacker français qui avait ralenti la diffusion du ransomware *Wannacry* en mai 2017. « *Il n'avait que le BAC. L'ANSSI a voulu l'engager mais ne pouvait pas vu les statuts. Il travaille depuis à Dubaï où il a été accueilli comme il se doit*.[612] » déplore Fabrice Epelboin, ajoutant qu'il n'y a pas de corrélation entre niveau de diplôme et expertise en hacking. Le collaborateur de l'ANSSI, « Bob », confirme les propos en parlant du besoin utilitariste en France concernant les hackers ; « *Le cadre légal existant est très prégnant. Il y a le problème de l'habilitation secret défense liée à ces métiers. Il y a un curseur, un juste milieu, même si les profils classiques sont privilégiés*.[613] »

L'on observe que la situation est très hétérogène. Même si la classe politique semble encore très étrangère aux questions cyber, plusieurs acteurs notent qu'il n'en va pas de même avec les SR qui, par pragmatisme et communauté de pratiques sont en mesure de comprendre l'état d'esprit des hackers. Selon Fabrice Epelboin, il y a « *un certain partage de valeurs avec les SR, mais ça se passe malgré le politique*.[614] » Le point de vue réflexif d'« Alice » vaut qu'on s'y penche : elle pense que le fameux et cryptique jeu de pistes baptisé « Cicada 3301 », créé en 2012, s'appuie sur le besoin d'identifier les profils de haut potentiel – pour les recruter – dans

[610] Entretien avec l'auteur, 27/02/2023. Bien qu'il souhaite rester indépendant, son projet n'a jamais été appuyé via des subventions publiques, alors qu'il suscite désormais un engouement international.
[611] Entretien avec l'autrice, 30/03/2022.
[612] Entretien avec l'auteur, 08/04/2022.
[613] Entretien avec l'auteur, 15/10/2021.
[614] *Ibid.*, 15/10/2021.

l'informatique en général et la cryptographie et l'OSINT en particulier. Selon « Alice », ce n'est pas la NSA, donc pas les États-Unis qui se cachent derrière le jeu. Pour elle, il pourrait s'agir tout simplement de la France. Et ça continuerait aujourd'hui. Si l'on considère que la France jouit d'un long passé et d'une expertise certaine dans la cryptographie, et possède l'une des communautés d'OSINTers les plus reconnues mondialement, son appréciation du phénomène n'est pas farfelue[615]. Si l'on conjugue approche secrète voire ésotérique et services de renseignement, le mythe supposé d'une cellule baptisée « Richelieu » au sein de l'État français confirme, en tout état de cause, la plausible convergence de pratiques avec certaines communautés de hackers.

- ***Dispositif opérationnel – 5e caractéristique : maîtrise de l'information via le triptyque acquisition–sécurité–influence***

Si ce cas est évoqué ici, c'est parce qu'il a été mentionné par certaines personnes interrogées dans le cadre de notre recherche. En effet, Alexandre Oda notamment évoque à plusieurs reprises cette « cellule Richelieu », cellule de renseignement spécialisée dans l'informatique qui aurait été mise en place pour favoriser la résistance aux cyberattaques. Un ancien du renseignement interrogé – que nous tiendrons secret – témoigne également d'une « cellule cyber » (non connue) entre EMA (État-major des Armées) et DGSE dédiée à la pénétration des SI. Alexandre Oda précise : *Nous la France on est très silencieux, on fait pas beaucoup de bruit, mais on n'est pas les derniers crois-moi.*[616] » Pour autant, *tamponné* et en lien avec la DGSE, contacté par le COMCYBER et ancien membre des forces spéciales de l'armée de Terre, Alexandre Oda ne semble pas en savoir davantage sur cet organisme.

Outre cet aspect équivoque, qu'en est-il de points mieux documentés sur les liens entre la classe politique et les hackers ? Si ces derniers « *sont ouverts d'esprit et faciles à appréhender* », selon Frédérick Douzet, « *l'intérêt lucratif est important, mais des signalements responsables sont réalisés. Ça reste ambigu avec par exemple un marché des vulnérabilités* », évoquant par-là les failles *zero-day* dont on a vu que Victor Poucheret estime que l'État français pourrait en acheter officieusement. Par ailleurs, « *il y a un encouragement du hacking dit éthique aujourd'hui* [via les] *concours et le bug bounty.* [L'État] *recherche des profils atypiques autodidactes désormais.*[617] » Victor Poucheret corrobore cet avis et loue la LPRN, « *qui ouvre la voie au hacking éthique. C'est une première valorisation du hacking que*

[615] Entretien avec l'autrice, 01/03/2023. https://fr.wikipedia.org/wiki/Cicada_3301. Une œuvre de fiction a même été dédiée à ce phénomène : *Dark Web: Cicada 3301*, de Alan Ritchson en 2021, prenant le parti de la tragicomédie.
[616] Entretien avec l'auteur, 09/07/2020 et 16/06/2021. L'on pourra se référer à ce témoignage *a priori* unique et sans gage de fiabilité : https://www.politique-actu.com/dossier/cellule-richelieu-renseignements/1686812/.
[617] Entretien avec l'autrice, 30/03/2022.

*l'on doit aux prédécesseurs, la génération précédente des hackers, de la "communauté", les Yogosha et consorts.*[618] »

Toutefois, ce versant positif est contrebalancé par des propos plus nuancés, lesquels mettent en avant le manque d'acuité et d'intelligence collective. Le LCL Leberon déplore notamment l'aveuglement des autorités politiques : « *En France, pour le renseignement, on n'a pas pris la mesure des enjeux.* [...] *Il n'y a pas de culture du renseignement ou du lobbying en France.* [...] *On a une myopie intellectuelle, pour tout. Le renseignement cyber devient presque gadget. C'est une source, et cette source devrait être exploitée, mais devrait venir après le partage transversal de l'information. Dans le public, il y a une prudence qu'il n'y a pas dans le privé. La place du public est assujettie au politique.*[619] » De son côté, Alexandre Papaemmanuel fustige une situation dans laquelle « *En France, beaucoup de contrats sont perdus dans le cyber.* [*Ce n'est*] *pas du tout l'approche des USA, dont la logique est celle d'un État-stratège géoéconomi*[qu]*e. Exemple : dans l'exploitation et l'analyse, Palo Alto a donné Palantir.*[620] » Des propos qui très certainement alimentent le constat d'un dispositif grandement perturbé en France, où le manque de vision stratégique nuit considérablement à nos intérêts de souveraineté et d'autonomie stratégique en termes de numérique.

- ***Dispositif opérationnel – 6e caractéristique : processus réticulaire via un dispositif intelligent***

Le propos est cinglant mais vécu :

> *« Il y a un retard et une non-adéquation entre les problématiques et le contexte actuels par rapport au fonctionnement administratif d'une manière générale en France. Le cadre juridique pose le problème de l'adaptation avec la communauté du hacking. Ce genre d'initiatives avec les éléments évoqués plus haut montre qu'on est sur la bonne direction en France. Mais il y a une question d'*upscaling *à faire. Et notamment, faire face à la lourdeur administrative incroyable ne serait-ce que vis-à-vis des appels d'offres publics. Ce n'est évidemment pas agile.*[621] »

Si les services de sécurité au sens large peuvent souvent aller dans le sens d'un partage des connaissances, l'appareil d'État semble en revanche accuser le coup. Est-il dès lors possible de bâtir un dispositif intelligent national digne de ce nom ? Christophe, officier de la DGSI peu loquace nous éclaire sur un point : « *Les dirigeants des SR ne se soucient pas du cyber.* » S'agissant du Cluster Data Intelligence du GICAT, qui associe plusieurs acteurs industriels français de la sécurité, ou encore sur Palantir, Christophe dit ne pas savoir si cela marche, mais

[618] Entretien avec l'auteur, 14/11/2021.
[619] Entretien avec l'auteur, 21/06/2017.
[620] Entretien avec l'auteur, 26/07/2017.
[621] Entretien avec Victor Poucheret, 14/11/2021.

que « *la concurrence est incontournable. Donc, la mutualisation difficile. Ça reste cloisonné entre domaines et secteurs d'activités*. [Il y a le] *problème des actionnaires. Les échanges/interactions entre entreprises et État* [sont] *fonction de leur savoir-faire respectif. C'est là qu'il y a un réseau*.[622] »

Les réseaux à proprement parler, les possibles synergies avec les hackers pourraient se constituer à partir des « *communautés de connaissance, en termes d'informations par contacts étroits et interrelations entre hackers, entreprises pratiquant l'IE et les SR d'État*. [...] *il y a aussi des communautés en termes de compétences, d'intelligence collective, en termes de ressources humaines* » avance Cédric Perrin, ancien officier de la DRSD. Ce dernier évoque en outre l'Intelligence Campus de la DRM qui participe à cette « *mise en communauté* [...] *avec l'idée d'une uniformisation* », tout en précisant que les acteurs qu'il réunit (universitaires, entreprises, administration) ne sont *a priori* pas en rapport avec des hackers. Il fait toutefois remarquer que « *dans le cadre des tables rondes, conférences, sensibilisations grand public sur la cybersécurité, il y a toujours plusieurs communautés représentées*. » Citant *Intellipedia*, la communauté numérique du renseignement américain, Cédric Perrin note que ça favorise « *le partage de pratiques, ce que l'on voit dans le monde privé et de l'entreprise en fait. Donc, on voit bien la mise en réseau, les interrelations, les croisements, l'hybridation… L'équivalent français est l'Académie du renseignement, même s'il n'y a pas, pas encore, la dimension numérique. Pas de plateforme numérique collaborative, mais un site web*.[623] » Mais il n'y a ici aucun rapport ni réseau intégrant des hackers même éthiques.

Enfin, l'exemple allemand avec le Chaos Computer Club (CCC) est incontournable, alors que plusieurs observateurs concernés interrogent la possibilité de disposer d'une telle tribune mettant en relation constructive hackers et autorités. Pierre Penalba concède au sujet du CCC : « *ça n'a pas été toujours rose, mais oui c'est positif et loin de ce qu'on a en France. Au début, ils avaient alerté en piratant une banque allemande et il y avait eu des frictions. Ensuite, ils ont réussi à s'imposer comme une interface qui discute avec l'État*.[624] » Selon Fabrice Epelboin, « *En France, il n'y a pas cette interaction. Mais des contacts entre État et individus. Pas de relations donc avec l'équivalent du CCC allemand*.[625] » Plus mesuré, Yassir Kazar temporise et réfléchit précisément au meilleur candidat pouvant former un CCC à la française : « *L'Allemagne est certes plus ouverte avec le CCC, qui s'est imposé, mais la relation suit une dynamique en France. En France, l'équivalent du CCC est l'association La quadrature du net, en lien avec la Hackerzvoice*.[626] » Mais à la question de savoir si cela pourrait favoriser la

[622] Entretien avec l'auteur, 03/07/2019.
[623] Entretien avec l'auteur, 05/10/2017.
[624] Entretien avec l'auteur, 07/07/2023.
[625] Entretien avec l'auteur, 08/04/2022.
[626] Entretien avec l'auteur, 20/05/2022.

structuration d'une communauté unifiée de hackers en France et la part de représentation de ces derniers au sein du pays, il avoue qu'il « *manque un organisme de représentation, comme le CCC. Ça devrait sans doute venir de la communauté française du hacking, mais il n'y a pas de groupes d'individus assez forts, avec un leadership portant des revendications sur la société et la politique, pour structurer la communauté. Cela peut-il venir du Parti pirate ?* » s'interroge-il à haute voix. « *C'est lié à La Quadrature. Hackers sans frontières ? Pourquoi pas, mais quelle dynamique réelle ? Mais elle a une vocation européenne, bien que ce ne soit pas contradictoire. Il y a trois acteurs dans le bug bounty en France : les deux premiers sont français : Hack in Provence* […] *et La quadrature du Net. Ce n'est pas à l'État de le faire.*[627] »

Au bilan, après avoir analysé ce cas, nous appliquons notre schéma basé sur l'analogie de la boussole.

| ***Boussole de disposition mentale* :** | | ***Boussole du dispositif opérationnel* :** |
|---|---|---|
| 1- Posture et intentionnalité |  | 5- Adaptabilité et transversalité |
| 2- Culture et intelligence | | 6- Méthodes et outils |
| 3- Patriotisme et souveraineté | | 7- Intégration et synergie |
| 4- Organisation et cohésion | | 8- Plasticité et agilité |

1- Citons les propos éclairants de Karim Lamouri, empruntant lui-même, de mémoire, à Sun Zi : « *En France, on s'ignore : on ne connaît pas les forces qu'on a. Synacktiv, qui a piraté Tesla, c'est bien beau, mais on focalise sur les évènements "com". C'est une goutte d'eau. Donc on ne se connait pas…*
*"Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites."*
*C'est, selon moi, la synthèse qui caractérise bien la France.*[628] »

2- Observateurs, spécialistes et hackers pointent en permanence le manque de culture cyber des autorités politiques. Pourtant, lorsqu'il s'agit des services de sécurité, il en

[627] Entretien avec l'auteur, 20/05/2022.
[628] Entretien avec l'auteur, 07/07/2023.

va autrement. À ce propos, Fabrice Epelboin évoque les anciens du renseignement. Citant TEHTRIS notamment, il explique : « *Soit ils montent leur affaire, ou alors ils vont travailler pour des entreprises du type GAMAM au moins quelques mois, pas par manque de patriotisme, mais parce que ça s'y prête et qu'ils ont le "mindset" compatible, ils sont ouverts d'esprit. Même les RH dans les entreprises classiques et notamment françaises n'ont pas le* mindset.[629] »

3- Bien que la réflexion sur la notion de souveraineté numérique date déjà de plus de vingt ans, il semble incongru que des missions d'information aient été menées par les parlementaires notamment en 2021. Si l'on considère les propos de Fabrice Epelboin, selon lesquels « *la France est très corrompue par les GAFAM* », ces manifestations d'intérêt semblent toutefois pertinentes et tomber à point. S'agissant de la cybersécurité brute voire de la cyberdéfense, Marc Sejean souligne que, de leur côté, « *les hackers d'aujourd'hui sont différents* [...] *et cette nouvelle génération est prête à défendre aussi bien qu'à attaquer pour leur pays.* [...] *C'est un travail bénévole, que les hackers n'ont pas toujours été prêts à fournir.*[630] » Suivi par Alexandre Oda, pour qui « *on aimerait aller plus loin, pouvoir attaquer ceux qui nous attaquent, peu importe le pays.*[631] » Marc Sejean poursuit et déplore : « *En France, il est toujours complexe de passer réellement à l'attaque.* [...] *C'est très compliqué, on est une démocratie, un État de droit, et on doit se battre contre des pays qui ont des structures moins monolithiques où il y a une perméabilité entre les services secrets, les mafias et les cybercriminels.*[632] » Alexandre Oda est un bon exemple de ce patriotisme pragmatique : « *patriote, mais pas naïvement, je me consacre à des activités légales,* [avec] *des convictions. Je mène des actions pour trouver des* grey *et des* black hats*, je donne tout aux autorités et ils font leur travail* [...]. *J'aide les entreprises mais je vais aussi chercher les méchants au fond de leur trou, parce qu'il faut aller chercher le mal à la base* [...]. *Pirater c'est interdit, mais derrière tu donnes des accès à des groupes, tu fais avancer des affaires d'Interpol, tu leurs donnes des éléments supplémentaires.*[633] » Mais ces initiatives personnelles sont-elles prises en compte, s'inscrivent-elles dans un cadre stratégique créé par l'État ? Problème soulevé par Fabrice Epelboin, lequel évoque les difficultés à structurer ces initiatives et intégrer ces forces vives : ***« Il y a des contacts avec les SR étatiques parce qu'il y a beaucoup de patriotes chez les hackers, mais c'est difficile à***

[629] Entretien avec l'auteur, 08/04/2022.
[630] Entretien avec l'auteur, 20/03/2023.
[631] Entretiens avec l'auteur, 09/07/2020 et 16/06/2021.
[632] Entretien avec l'auteur, 20/03/2023.
[633] *Ibid.*, 09/07/2020 et 16/06/2021.

***structurer car on passe juste par des individus.*** **»**, même si « *les SR* [...] *emploient* [...] *des hackers et* [...] *comprennent le langage et le savoir-faire de la communauté.*[634] »

4- Il manque par conséquent un liant entre les services de sécurité et les hackers, et d'une réelle interface entre ces derniers et les autorités politiques. Plusieurs témoignages ont pointé des pratiques archaïques d'entre-soi, et Karim Lamouri, dont les mots sont durs, ne dit pas autre chose : « *Il y a des rapports de pouvoir et d'argent dans la cybersécurité.* » Et de citer par exemple ce qu'il assimile à des liens d'intérêt (y compris financier, participation...) entre l'État et Orange Cyberdéfense. Il dresse un tableau très noir de la classe politique, soutenant qu'« *au niveau des élites politiques, il n'y a pas d'intérêt à défendre la nation. Mais seulement "à se placer", avec leurs familles et leurs proches. Il n'y a pas de lumière. Le salut viendra de la province !*[635]» Ces propos, en creux, interrogent sur la dimension plus générale de la cohésion nationale en France. Plus positif, ceux de Guillaume Poupard tranchent mais questionnent aussi la possibilité de dépasser certains verrous juridiques et politiques. L'ancien directeur de l'ANSSI parle d'une « *belle évolution dans la perception des choses, la nécessité d'un échange et d'une coopération. On ne cherche pas forcément à savoir d'où viennent les infos. Après, la question est : il y a ceux qui respectent la loi et les autres.* » Guillaume Poupard dit avoir ouvert au maximum autour de l'écosystème mais a fixé une ligne rouge avec les gens non respectueux de la loi. « *Or,* poursuit-il, *la loi française est très stricte. Donc un chercheur en informatique est toujours limité. Car un hacker éthique, ce n'est pas un "blanc" pur. Rapprocher les compétences, avoir une bonne image pour le recrutement... ça passe beaucoup par les connaissances. Donc s'ouvrir à tout l'écosystème cyber, à la communauté open source, l'enseignement, tant qu'ils ne franchissent pas la ligne rouge.* [Ces acteurs se] *rencontrent tant qu'ils ne passent pas cette ligne.*[636] »

5- Si la classe politique semble montrer des signes de préoccupation et pour certains élus un investissement manifeste, les positions restes encore très arcboutées sur des principes désuets et un immobilisme important. Les initiatives souvent personnelles certes parfois élargies à une logique transpartisane sont louables, mais peinent à fédérer l'ensemble de la classe politique. Les progrès buttent en effet sur la difficulté à passer un cap d'ordre culturel, qu'il s'agisse des questions de souveraineté numérique qui touchent à des phénomènes d'aveuglement cognitif général, ou de

[634] Entretien avec l'auteur, 08/04/2022.
[635] Entretien avec l'auteur, 07/07/2023.
[636] Entretien avec l'auteur, 17/04/2023.

prise en charge sérieuse et globale des risques de cybersécurité, posant la question de l'intégration des hackers. Prenons pour exemple les propos de Guillaume Poupard sur la position novatrice et courageuse de la Belgique à ce sujet. Ce dernier s'interroge : « *En Belgique, il y a bien une libéralisation de l'approche bug bounty. Pourquoi cette mentalité différente de celle de la France, même si c'est récent ? C'est un plus petit pays, plus facile à gérer ? Je ne suis pas trop pour en France. Bien sûr, il y aurait un effet pervers. On est choqué ici de cette approche belge parce qu'on a peur que des failles soient découvertes par des "méchants". Il vaut mieux un encadrement*.[637] »

6- Les hackers partagent avec les autorités de sécurité des pratiques communes avant tout unifiées par l'outil informatique. C'est par exemple ce qui fait dire à Marc Sejean que « *la jonction entre le monde civil et militaire est, de nos jours, assez fine* »[638]. On l'a vu, les observateurs et spécialistes parlent de convergence technique par le contenant. Néanmoins, s'il y a communauté de pratiques, y a-t-il communauté d'intérêt ? L'on peut d'abord répondre positivement à cette question dans la mesure où les témoignages recueillis dénotent des valeurs communes comme le patriotisme. Mais aussi négativement : d'une part, ce n'est pas toujours le cas car la solidarité a ses limites et les statuts de chaque « communauté » diffèrent en droit et souvent en nature. D'autre part, là où les pratiques et certaines valeurs peuvent être partagées avec une partie du personnel de ces services de sécurité, les élites politiques, elles, y sont pour une très large majorité étrangères. Pour reprendre les mots d'Éric Filiol, constituer une réserve citoyenne de cyberdéfense avec des énarques ou des normaliens ne va pas particulièrement contribuer à renforcer la sécurité numérique nationale.

7- Comment considérer intégrer les hackers dans une politique publique de cybersécurité si les élus peinent à comprendre leur plus-value et leur état d'esprit ? Sans interface de dialogue entre hackers et État, « *il n'y a donc pas de structuration, alors qu'avec le Chaos Computer Club, ça existe en Allemagne. Le Hack, donc HackerzVoice, pourrait jouer ce rôle avec les plateformes de bug bounty*.[639] » propose Guillaume Poupard. Si, de son côté, Yassir Kazar voit juste, alors les hackers pourraient aussi prendre les devants et édifier cette interface avec les autorités. Les volontés ne manquent pas du reste comme le dit Marc Sejean : « *On est une nouvelle génération de hackers, la plupart sont patriotes et prêts à aider les TPE et les forces*

[637] Entretien avec l'auteur, 17/04/2023. Rappelons tout de même que la loi belge en question encadre bien lesdites pratiques et que les remontées de vulnérabilités doivent notamment passer à un moment ou un autre par l'homologue de l'ANSSI, le CCB (https://ccb.belgium.be/).
[638] Entretien avec l'auteur, 20/03/2023.
[639] Entretien avec l'auteur, 17/04/2023.

*de l'ordre à sécuriser le pays*.[640] » Quant à parler de synergie, la voie est encore à tracer comme en atteste Victor Poucheret : « *Les hackers et l'État ne communiquent que peu, c'est ponctuel sur un sujet précis, ou via les appels d'offres publics indirects*.[641] »

8- Dans la droite ligne des propos de Victor Poucheret cités plus haut, l'agilité n'est pas ce qui caractérise les relations entre les autorités et les hackers. Si les associations propres aux hackers et leurs communautés de partage sont extrêmement dynamiques, il n'en va bien sûr pas de même pour les structures du pouvoir étatique. Est-ce pour autant une fatalité ? Rappelons les paroles de l'entrepreneur Jean-Nicolas Piotrowski sur l'absence de toute stratégie au niveau de l'État.

## Caractéristiques-clés – synthèse et hypothèses

Quels enseignements tirer de ce cas à partir des caractéristiques-clés, et ce dernier répond-il à nos hypothèses de recherche ?

• L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)

• L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)

• L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

### Synthèse :

L'analyse des corpus documentaires législatifs (missions d'information, débats parlementaires, projets de loi) témoigne globalement d'une incompréhension encore manifeste du rôle et de la plus-value des hackers éthiques chez nos élus. Pour cette étude, forcément partielle, des rapports qu'entretiennent la classe politique en général et les hackers, il est possible de tirer quelques enseignements :

- D'abord, la classe politique est très éloignée, à de rares exceptions près, du monde du numérique qui pourtant de manière fulgurante et permanente refaçonne nos perceptions et la réalité dans laquelle nous évoluons. Si la cohérence politique fait

[640] Entretien avec l'auteur, 20/03/2023.
[641] Entretien avec l'auteur, 14/11/2021.

probablement déjà défaut, comment dès lors assurer une cohésion à même de nous assurer la meilleure résilience face à cette réalité perturbée ? Les hackers forment sans nul doute un chainon essentiel de la « République numérique » car ils sont à la fois des innovateurs et des sentinelles dans les mutations technologiques.

- Par ailleurs, si les services de sécurité ont le plus souvent des appétences communes, utilisent les mêmes outils que les hackers et ont une grande conscience de l'importance de la sécurité de l'information, cela ne suffit pas à garantir des valeurs partagées à même de solidariser les deux mondes. Plus préoccupant, le manque de culture stratégique et informationnelle des élites politiques françaises, du moins l'hétérogénéité flagrante de leur niveau collectif d'une conscience de sécurité numérique, entrave fortement leur capacité à gouverner et légiférer « en connaissance de cause », face aux réalités du terrain. Les initiatives individuelles sont à saluer, mais ne permettent pas « d'entrer ensemble en stratégie ».

- Enfin, si certains réseaux existent, ils sont plus volontiers établis entre acteurs publics et organisations privées « d'ascendance » et d'ordre régaliens, mais certainement pas réellement entre autorités politiques et hackers. Une passerelle pourrait être jetée par le truchement des services de sécurité du pays, mais cela suppose un déverrouillage et un désilotage d'abord cognitifs puis organisationnels du politique, et la fin d'une défiance de plus en plus incongrue vis-à-vis de hackers par définition adaptables et agiles.

### Rappel des hypothèses :

1 – ces trois mondes (hackers–État–entreprises) sont intégrés et dans une co-construction (interaction et communication décloisonnées, projets communs, logique de dispositifs intelligents, synergie…)

2 – ces trois mondes sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas (incommunication) par manque de synergie

3 – ces trois mondes s'ignorent (acommunication)

Eu égard à cette étude de cas révélant les lents progrès réalisés par les politiques au moins à titre individuel, progrès à replacer néanmoins face au constat d'un manque évident d'intégration des hackers dans un projet stratégique, nous pouvons privilégier la validation de l'hypothèse n°2.

### Résumé de l'étude de cas :

S'agissant de ce deuxième cas, en lien avec cette fois le regard politico-législatif porté sur les hackers, l'on retiendra qu'il **vient conforter les leçons tirées de l'affaire relative au premier cas, puisque des aménagements législatifs corrigent l'étroitesse de la loi en la matière. Tout en laissant, cependant, encore un flou règlementaire dû à la difficulté pour la classe politique à comprendre réellement l'utilité de considérer les hackers comme des piliers de la cybersécurité**. Sans hackers, qui pour faire remonter les failles et les tester, hormis des spécialistes de sécurité informatique dont le métier est la recherche, les RSSI ayant évidemment déjà bien à faire pour sécuriser leur propre organisation ? La classe politique est bien consciente du risque cyber mais n'a qu'une faible culture dans le domaine. Elle est souvent, à l'image du grand public, happée par les aspects fascinants et tendanciels des technologies numériques. Malgré tout, le niveau de cette inculture cyber n'est pas homogène et certaines initiatives individuelles sont à saluer, qui proposent des projets encourageants. Eu égard à ces considérations, nous avons validé l'hypothèse n°2.

**Figure 39 :** *Tableau récapitulatif de l'étude de cas n°2*

| ***Boussole de disposition mentale :*** | **Bilan −/± (classe politique) ; Bilan + (certaines entreprises)** |
|---|---|
| 1- Posture et intentionnalité | • Manque de connaissance de ses propres forces de la part de l'État<br>• Absence de vision stratégique |
| 2- Culture et intelligence | • Manque de culture cyber et de sécurité chez les élites politiques<br>• Au contraire des anciens des SR qui créent leur entreprise<br>• Entreprises françaises généralement peu acculturées elles aussi. |
| 3- Patriotisme et souveraineté | • Intérêt et inquiétudes (tardifs et épisodiques) pour la souveraineté numérique chez les politiques<br>• Pas de cadre stratégique étatique pour accompagner la posture patriotique de nombreux hackers et leur volonté d'agir<br>• Contacts entre SR et hackers mais non structurés et seulement à titre individuel |
| 4- Organisation et cohésion | • Manque de liant et d'une interface entre hackers et autorités<br>• Verrous juridiques et politiques, voire conflits d'intérêts chez les élites |
| ***Boussole du dispositif opérationnel :*** | **Bilan ± (classe politique) ; Bilan ± (forces de sécurité)** |
| 5- Adaptabilité et transversalité | • Immobilisme important chez la classe politique<br>• Mis à part certains acteurs et initiatives individuelles |
| 6- Méthodes et outils | • Communautés de pratiques entre civils/militaires, hackers/forces de sécurité (convergence technique)<br>• Communauté d'intérêt en revanche relative : patriotisme commun avec les forces de sécurité, valeurs moins évidentes chez les politiques. |
| 7- Intégration et synergie | • Pas de structuration d'une interface de dialogue entre hackers et politiques<br>• Mauvaise compréhension de la plus-value des hackers chez les élites politiques<br>• Pas de synergie avec l'État, communication ponctuelle avec les hackers |
| 8- Plasticité et agilité | • Lourdeur des structures du pouvoir politique<br>• Absence de stratégie au niveau de l'État pointée par de nombreux interviewés |

### 3) Les hôpitaux français ciblés par les cyberattaques : des carences financières et sécuritaires manifestes

*« L'ambiance à l'hôpital était cauchemardesque. On pense à l'administratif, mais il y a également tous les services de pharmacie. Sans ordinateurs, il n'y avait plus la possibilité d'avoir une traçabilité sur les dosages des médicaments, sur les préparations de chimiothérapie. Les automates des laboratoires ne fonctionnaient plus, donc plus de possibilité de faire les analyses biologiques. Toute l'activité s'arrêtait. L'hôpital n'avait plus moyen de fonctionner.*[642] »

Francine Corneux,
coordinatrice des secrétariats médicaux
de l'hôpital de Corbeil-Essonnes.

Depuis le début de la décennie, on assiste à une recrudescence globale de la cybercriminalité avec des cyberattaques portées notamment contre des organismes publics : OSE/OIV, puis collectivités locales et centres hospitaliers. Cette séquence s'inscrit par ailleurs dans les contextes de la pandémie et de la guerre russo-ukrainienne débutée en février 2022 et suivie des tensions diplomatiques opposant la Russie et l'Europe. Des rapports de force idéologiques et informationnels renouvelés se font jour entre l'Occident et des régimes autoritaires, et des hackers-corsaires russes, souvent cachés derrière des organisations jusqu'ici sans drapeau et réputées cybercriminelles, n'hésitent plus à revendiquer ouvertement des objectifs de cyberguerre et leur collusion avec le Kremlin.

À partir de 2020 et plus encore 2022, une vague de cyberattaques plus ou moins abouties vise les établissements de santé français. Plusieurs plans blancs sont déclenchés pour détourner rapidement les flux de patients vers d'autres centres hospitaliers. La désorganisation est telle que les établissements sont entièrement paralysés : urgences, ressources humaines, gestion des plannings, équipements et matériels, fichiers des patients et des personnels, téléphonie parfois… C'est le retour à des conditions spartiates et archaïques de travail. Il faut en moyenne entre 12 et 18 mois à ces institutions pour se remettre de la crise. Il faut dire que les données de santé sont soit particulièrement lucratives pour les cybercriminels[643], soit une cible de choix à fin de déstabilisation pour les États qui pratiquent la cyberguerre et les coups de main opportunistes.

[642] https://www.radiofrance.fr/franceculture/podcasts/les-pieds-sur-terre/cyberattaques-7095850.
[643] Un rapport de la société américaine BreachQuest indique que les données de santé sont les plus lucratives, un dossier médical se revendant 350$, un prix cinquante fois plus élevé qu'un dossier bancaire (https://www.breachquest.com/app/uploads/2022/05/BQ-Healthcare-Report.pdf).

### a) *Des cibles de choix particulièrement vulnérables*

L'ANSSI fait part qu'après les PME et les collectivités territoriales, les établissements hospitaliers forment la troisième cible privilégiée par la cybercriminalité[644]. Ainsi, pour prendre la mesure de la menace que constituent les cyberattaques contre les centres de santé, prenons la liste de ceux qui ont été touchés en 2022 :

- Clinique Léonard de Vinci de Chambray-les-Tours : *attaque par ransomware le 7 janvier. Les malfaiteurs ont demandé 500 000 euros de rançon.*
- Cité sanitaire de Saint-Nazaire : *attaquée le 12 janvier, les patients sont privés de télévision, d'Internet et de communication avec leurs proches.*
- Hôpital de Castelluccio, Ajaccio : *touché par un ransomware le 28 mars, les soins de radiologie et oncologie étaient suspendus.*
- Hôpital de Saint-Dizier et de Vitry-le-François : *victimes d'un ransomware le 19 avril. Les auteurs exigeaient une rançon de 1,2 million d'euros.*
- Centre hospitalier de Mâcon : *touché le 27 mai.*
- Centre hospitalier de Corbeil-Essonnes : *attaque par ransomware le 20 août, revendiquée par LockBit. Demande de rançon de 1 million d'euros.*
- Hôpital de Cahors : *cyberattaque le 12 septembre.*
- Maternité des Bluets, Paris-XIII[e] : *touchée par un ransomware le 9 octobre, revendiqué par Vice Society.*
- Hôpital André-Mignot, Versailles : *attaque par ransomware le 3 décembre.*
- Centre hospitalier d'Argenteuil (déjoué) : *tentative d'intrusion début décembre.*
- CHU de Nice (déjoué) : *touché le 3 décembre, le pare-feu a bloqué l'opération*[645].

Comme on peut facilement en juger, le nombre de centres de santé touchés est important. Or, en dépit des messages rassurants de plusieurs groupes cybercriminels, il s'avère que ces derniers pratiquent le mensonge en plus du cynisme le plus strict. À l'image de l'un des gangs russes les plus sinistrement connus, *LockBit*, qui a l'habitude de revendiquer ne pas vouloir attenter à la vie des usagers à travers ce slogan : « *Il est interdit de mettre en jeu la vie des patients, mais parfaitement autorisé de voler des données à un hôpital* »[646].

[644] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
[645] https://www.numerama.com/cyberguerre/1219264-cyberattaque-la-liste-des-hopitaux-touches-en-2022.html. Les hôpitaux ne mentionnent pas toujours les types et vecteurs d'attaques ayant été utilisés contre eux.
[646] https://www.numerama.com/cyberguerre/1177180-un-hacker-russe-membre-du-celebre-groupe-lockbit-a-ete-arrete-au-canada.html

Selon un rapport de l'ANSSI, l'année précédente a été pire puisque, chaque semaine en 2021, un incident de ce type avait lieu dans un établissement hospitalier français[647]. La figure ci-dessous répertorie les chiffres-clés pour les années 2021 et 2022.

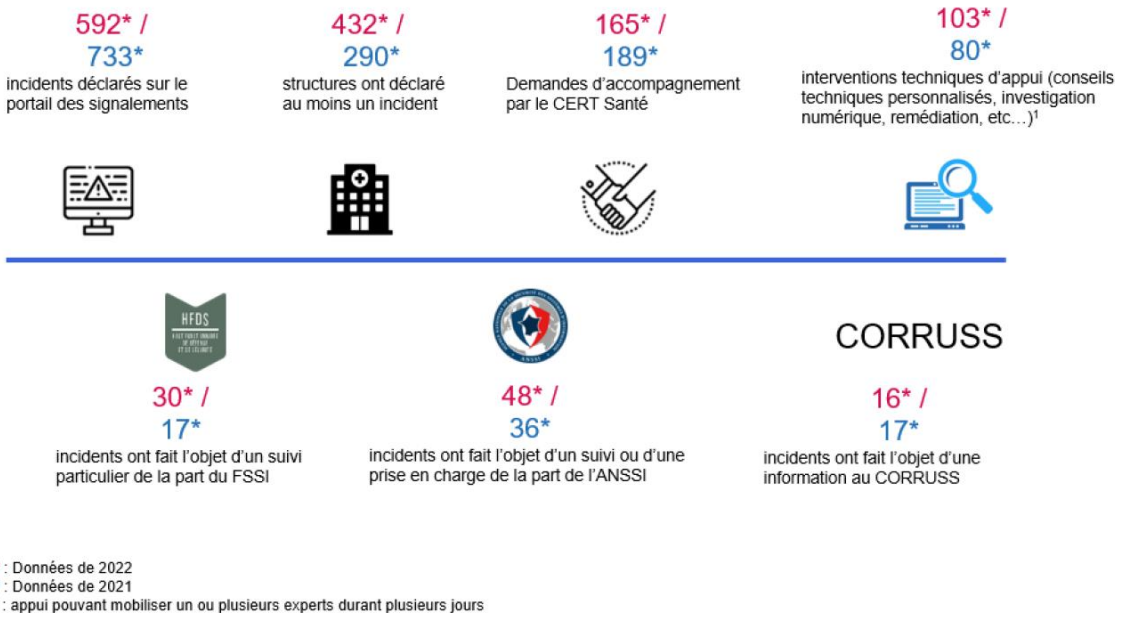



**Figure 40 :** *Chiffres-clés des cyberattaques visant des centres de santé (2021-2022)*

Source : Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social – Rapport public 2022, Agence du numérique en santé (ANS)/CERT Santé[648].

Ainsi, malgré un dispositif spécial mis en place dans le cadre du plan de relance post-Covid, le soutien de l'ANS et du CERT Santé et des plans de renforcement de la cybersécurité des Agences régionales de santé (ARS), rien n'y fait et les hôpitaux semblent impuissants. Comment dès lors expliquer cet état de fait ? En janvier 2023, une conférence dédiée à ce sujet qui s'est tenue dans le cadre du FIC de Lille répond en partie à la question. Les intervenants s'appuient sur le rapport de l'ANSSI et évoquent en premier lieu les « *dizaines de milliers de postes fonctionnant sous Windows XP, des appareils médicaux achetés dans les années 90 ou 2000* » qui équipent les hôpitaux français[649]. Ceci démontre que les centres de santé sont dotés de systèmes d'exploitation aux versions obsolètes et dont, par conséquent, les mises à jour de sécurité ne sont plus assurées. Du pain béni pour tout pirate informatique. Mais les failles s'avèrent avant tout d'origine humaine. Au-delà des aspects purement techniques, la situation

[647] https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
[648] https://esante.gouv.fr/sites/default/files/media_entity/documents/ans_certsante_rapport_public_observatoire_signalements_issis_2022_vf.pdf.
[649] https://www.usine-digitale.fr/article/cyberattaques-contre-les-hopitaux-la-question-n-est-pas-de-savoir-si-cela-va-arriver-mais-quand.N2092896 ; https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf.

appelle donc à un changement d'ordre culturel pour ces établissements dont les personnels sont peu habitués à gérer collectivement ce type de risque, dévolu à leurs yeux aux seuls « *gars de l'informatique*.[650] »

### b) *Des retours sur expériences révélateurs de la fragilité et du manque d'acculturation des hôpitaux à la cybersécurité*

Or, la situation est d'autant plus inquiétante que les objets connectés médicaux, la télémédecine et les systèmes et services de soins sont de plus en plus interconnectés. Certains ont du reste un impact direct avec la vie des patients puisqu'on parle de pacemakers connectés, de pompes à insuline téléopérées, sans parler des conséquences de gravité moindre mais tout à fait déstabilisatrice comme la prise en charge administrative des actes de soins dont la numérisation a rendu totalement dépendants les personnels de santé, avec les ruptures d'activité que cela suppose en cas de paralysie électronique.

Pour prendre la mesure du dénuement des centres de santé et de leur manque de culture de sécurité numérique, prenons les résultats d'une série d'audits réalisés bénévolement par Hackers Sans Frontières (HWB) auprès de trois hôpitaux français[651]. Quelles conclusions en tirer ? Les personnels soignants cochent malheureusement toutes les mauvaises cases ; pour résumer : absence de politique – ou de pratique – de gestion de droits d'accès informatiques (dont postes à sessions d'administrateur par défaut) ; procédures d'authentification inexistantes ou insécurisées : identifiants et mots de passe communs (parfois mentionnés ou « codés » sur des post-it[652]), comptes génériques pour la manipulation des progiciels métiers et logiciels plus courants ; absence de politique de proxy (reverse proxy[653]) ; pare-feu non configuré pour le filtrage ; aucune gestion des périphériques de stockage (clés USB issues de l'extérieur de l'établissement) ; budgets financiers DSI et *a fortiori* SSI, ainsi que ressources humaines faibles ; outrepassement de droits d'accès (par usure de l'activité métier) ; sécurité physique inexistante (infiltration aisée, dispositifs d'accès par défaut/non renouvelés) ; sensibilisation de la part des équipes SSI quasi-inexistante. Comme le mentionne HWB, ces trois cas ne sont pas forcément représentatifs du niveau de sécurité de tous les centres de santé, et il ne s'agit pas de blâmer des personnels mis à rude épreuve depuis des années de périclitation des services publics. Toutefois, il est à noter qu'en présence même de responsables de sécurité des SI (RSSI), ces hôpitaux restent impuissants. En effet, cette donnée revient régulièrement, comme nous allons le voir à travers les retours d'expérience (retex) réalisés par

[650] https://is.gd/XcCZS7 (lien contracté, 10/10/2023), dirigeant vers un article posté sur LinkedIn par Florent Curtet).
[651] Voir annexe 1.
[652] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 168.
[653] En substance, un proxy peut assurer le filtrage du SI vers l'internet ; un reverse proxy peut être configuré à l'inverse pour filtrer les accès distants provenant de l'extérieur vers le SI de l'hôpital.

trois établissements médicaux à Dax, Corbeilles-Essonnes et Villefranche-sur-Saône. Ces retex sont des initiatives très encourageantes et positives dans le sens où les centres victimes font, d'une part, une auto-analyse et s'acculturent naturellement à la cybersécurité, d'autre part partagent leur expérience – douloureuse mais formatrice – auprès des autres établissements de santé du pays.

Le Centre hospitalier de Dax a été attaqué le 9 février 2021 et a effectué un retex un an plus tard, le 18 mars 2022[654]. Il se résume à partir des mots mêmes de la direction du centre : « *Ce retour d'expérience à date anniversaire, a été réalisé afin de faire prendre conscience des impacts concrets d'une telle attaque sur les missions essentielles d'un centre hospitalier. Plus d'un an après, si le cyclone et la tempête sont dernière nous, il reste des stigmates forts*. » L'hôpital a en effet été touché par un rançongiciel de type *Cryptolocker* qui a chiffré 85% des serveurs (sur 150), mais n'a fait l'objet d'aucun vol de données. Il lui a fallu plus d'un an pour s'en remettre. À l'époque, la téléphonie et l'informatique ont été complètement paralysées ; les services de stérilisation, chimiothérapie, radiothérapie, et le stockage de l'imagerie étaient inopérants. Fait notable, les sauvegardes de données ont été également impactées et donc chiffrées par le *malware* ; ce qui prouve que la recommandation d'isoler les dispositifs de sauvegarde n'a pas été appliquée[655]. L'hôpital a fait appel à l'ANSSI, Orange Cyberdéfense ainsi qu'à l'ARS, et a avisé le SAMU local de limiter l'afflux de patients vers le service d'urgences. L'impact financier après un an a été estimé au total à 2 356 000€, qui ont fort heureusement été pris en charge par l'ARS.

Quels enseignements ont été tirés par le Centre hospitalier de Dax ?

- une cyberattaque dépasse une simple crise informatique.
- « *où l'intelligence collective et la débrouillardise permettent de sauver les meubles*. »
- certains logiciels sont changés car non compatibles avec l'infrastructure réseau.
- « *prise de conscience de notre vulnérabilité numérique (les anciens plus agiles que les jeunes ?) et obligation d'investir dans la sécurité informatique (compétences, investissements, prestations de sécurité*). »
- un SI renforcé, des règles de sécurité renforcées.
- un accélérateur de déploiement des solutions (sécurité et mise à jour des versions d'OS).

[654] https://web.archive.org/web/20230124083440/https://aime-et-partage.anap.fr/lanap-aime-et-partage/cyberattaque-au-ch-de-dax-1-an-apres ; La présentation du retex peut être consultée sur : https://fr.linkedin.com/posts/adusonchet_retex-cyberattaque-ch-dax-activity-6957346875788136448-CSjj, consulté le 10/09/2023.

[655] Cette préconisation est faite par l'ANSSI depuis seulement quelques années (quatre ans au maximum). Le MOOC de l'ANSSI sorti en 2017 ne faisait pas mention de ce risque lié aux connexion et automatisation des sauvegardes (https://secnumacademie.gouv.fr/).

Il faut noter qu'en dépit de la présence d'un poste de RSSI, il est mentionné le besoin en compétences et prestations de sécurité, à savoir de sous-traitance/accompagnement externe. Ce point mis en avant paraît incongru, les RSSI étant des experts de la sécurité informatique qui ont suivi un cursus spécialisé dans ce sens.

Qu'en est-il du Centre hospitalier sud-francilien de Corbeil-Essonnes (CHSF) ? Pour sa part, ce dernier a été attaqué dans la nuit du 20 au 21 août 2022 par *LockBit 3.0*, rançongiciel bien connu déployé par le groupe cybercriminel russe éponyme. Cette fois, l'établissement a été victime d'un vol de données en plus de leur chiffrement. L'entrée et en même temps vecteur d'attaque s'est avérée être une faille chez l'un des hébergeurs web de l'hôpital[656]. La demande de rançon prendra une voie inhabituelle qui a sans doute été le fruit d'un jeu sarcastique de la part du *ransomgang* : après quelques jours les imprimantes se sont en effet mises à éjecter un raz de marée de feuilles parmi lesquelles l'une portait la revendication. Elle s'élève à 10M$, qui n'ont pas été payés par l'établissement, tandis que les pirates ont alors diffusé toutes les données aspirées sur le *darkweb*. Le RSSI a été secondé et l'établissement accompagné par l'ANSSI et les entreprises Wavestone et MGM. Selon le retex, l'hôpital était très en dessous du niveau de sécurité requis pour un centre de soins. Une récupération des logs (journaux d'activités) a pu être assurée en vue d'identifier le niveau de la compromission et le vecteur d'attaque (non précisés)[657].

Voici les enseignements qui ont été retenus :

- une vraie politique de management de la sécurité a été instaurée.
- importance de travailler ensemble entre acteurs de la cybersécurité.
- besoin d'un large éventail de compétences.
- aspect collaboratif entre acteurs déterminant (« l'union fait la force »).
- recommandation pour améliorer la résilience des systèmes de sauvegardes, des systèmes de logs pour faciliter les investigations numériques *post-mortem* (forensique).
- nécessité de s'appuyer sur quelqu'un en interne ou sur un prestataire externe.
- prendre conscience de la SSI, faire un état des lieux (audit).
- nécessité de se préparer, anticiper, mettre en place une procédure de gestion de crise, renforcer le SI.

[656] Florent Curtet, *Hacke-moi…*, *op. cit.*, pp. 169-170.
[657] Retex publié sur le média social YouTube (https://www.youtube.com/watch?v=SqNALztVz1Y).

Encore une fois, les conclusions préconisent l'appui de prestataires externes ou internes ultraspécialisés, en dépit de la présence d'un expert en sécurité informatique (RSSI).

Enfin, observons le cas du Centre hospitalier de Villefranche-sur-Saône dont 400 serveurs réels et virtuels hébergés sur deux datacenters (avec un total de 3200 postes de travail) ont été également victimes d'un *ransomware*. L'impact a été moindre, les sauvegardes du SI n'ont pas été impactées, mais l'ANSSI, l'ARS et la MGM ont été sollicitées pour aider à une remédiation d'une durée de deux mois[658]. Malgré les sauvegardes épargnées, le centre a suivi les conseils de ses soutiens en procédant à la reconstruction complète de l'architecture informatique/réseau plutôt que de restaurer simplement son système. La décision a été prise en conscience en dépit du temps supplémentaire requis et bien que cela paraissait délicat. Il n'est pas fait mention de la présence d'un RSSI, et il semble que seul un DSI assurait la gestion du parc informatique. Les enseignements se résument à l'élaboration et l'exécution de nouvelles règles de sécurité, sans compter l'intérêt d'être appuyés par les organismes ou entreprises spécialisés lors de la crise.

Au bilan, les deux premiers établissements indiquent que la présence d'un RSSI n'a pas suffi et évoquent le besoin de compétences, donc de profils plus aguerris. Il faut toutefois faire remarquer que, d'une manière générale, les RSSI se plaignent – non dans ces retex où ils semblent se présenter eux-mêmes comme faisant partie des victimes – de manquer de ressources financières et de considération. Victor Poucheret fait part d'une anecdote dans ce sens et évoque le RSSI du CHU de Brest : « *Un an en poste, et il en a déjà marre. Comme dans bien d'autres organisations, il y a un cruel manque de ressources allouées à la sécurité informatique*.[659] » En effet, c'est aussi là que le bât blesse. Une étude du cabinet BreachQuest indique que le budget réservé à la cybersécurité dans les hôpitaux oscille entre 4% et 7% seulement du budget total réservé aux TIC, eux-mêmes poste de dépenses parmi d'autres[660]. En outre, le chiffre de 5% concernant les Centres hospitaliers français revient souvent dans les échanges sur le réseau socionumérique professionnel LinkedIn, chiffre que nous tirons de notre veille cybersécurité. Selon Karim Lamouri et pour avoir un référentiel sur le niveau moyen du budget des organisations, dans le monde privé 10% sont consacrés en moyenne à l'informatique et la SSI ; « *Ce qui est beaucoup pour des entreprises*. » Tandis que 2,5% à 3% du budget y sont consacrés (budget investissement plus fonctionnement) dans le secteur public. « *C'est un investissement donc il y a deux écoles, les entreprises qui investissent et*

[658] *Idem* (https://www.youtube.com/watch?v=lignfJXw8QI).
[659] Entretien avec l'auteur, 14/11/2021.
[660] https://www.breachquest.com/app/uploads/2022/05/BQ-Healthcare-Report.pdf. L'étude porte sur les centres de santé américains, possiblement mieux protégés. Dans un post LinkedIn, Florent Curtet fait par ailleurs valoir que le niveau de sécurité entre cliniques privées et établissements publics en France est sensiblement le même (voir annexe 1).

*comprennent qu'il faut anticiper et être résilient, donc comprennent que c'est un investissement et pas un gain direct ; et les autres.*[661] »

### c) *Clé de lecture du cas d'étude*

Cette brève étude a permis de dégager des tendances dans le rapport qu'entretiennent les centres de santé avec la cybersécurité. Deux principaux problèmes sont mis au jour grâce aux retours d'expérience que pratiquent désormais de plus en plus d'établissements victimes et aux audits souvent gracieux que réalisent certaines organisations de hackers (HWB, Yogosha…). D'abord, le manque d'acculturation aux questions cyber et risques numériques, aux pratiques d'hygiène informatique en particulier des personnels soignants. Ensuite, les carences budgétaires dont les équipes d'informatique et de SSI sont victimes, avant de subir la double peine du fait des cyberattaques. En somme, la synergie des moyens humains n'est pas de mise en anticipation, mais seulement en réaction à une crise.

- ***Disposition mentale – 1ère caractéristique : la complexité du réel et du « village global »***

On ne saurait incriminer directement les centres hospitaliers pour l'attention relative qu'ils portent aux questions de sécurité. Toutefois, et les retex le montrent très clairement, les leçons apprises de ces attaques ont tendance à faire prendre conscience des enjeux cyber et des conséquences néfastes qui découlent de celles-ci. La priorité, et c'est bien normal, est focalisée sur le soin. Mais ne pas se prémunir, c'est risquer de ne plus pouvoir soigner dans les meilleures conditions. Malgré la mise en place de plans dédiés à leur sécurité par les autorités publiques, les hôpitaux ne semblent pas suffisamment protégés y compris techniquement. Les directions et personnels d'hôpitaux s'investissent, contraintes par la force des choses à adapter leurs activités en prenant en compte cette nouvelle dimension qui ne relève pas seulement de l'équipe de l'informatique.

- ***Disposition mentale – 2e caractéristique : culture de l'intelligence rusée***

On l'a dit et induit à plusieurs reprises : les responsables de sécurité des SI qui occupent pourtant un poste titulaire dans les Centres hospitaliers ne semblent pas en mesure d'enrayer les cyberattaques. Ils ne sont pas non plus à blâmer compte tenu du manque de sensibilisation des personnels soignants et eu égard à leur faible budget. Toutefois, la mention récurrente de la nécessité de disposer de prestataires externes est explicite : un autre type de spécialiste semble tout désigné, il s'agit bien évidemment de hackers dont le mode d'approche est

[661] Entretien avec l'auteur, 07/07/2023.

précisément porté vers l'attaque, la ruse et l'approche indirecte. Les études et lesdits retex montrent bien que la menace évolue sans cesse et que les pirates informatiques sont de plus en plus aguerris, d'autant que croisés avec les activités classiques de cybercriminalité, des objectifs de cyberguerre viennent envenimer et complexifier les enjeux de sécurité des établissements. En attestent les revendications décomplexées de hackers-corsaires russes dont certains groupes jusqu'ici cantonnés à la criminalité font état de leur connivence directe avec le Kremlin. Citons notamment les groupes *Conti* et *LockBit*, qui servent désormais officiellement les buts de *contestation* voire d'*affrontement* du gouvernement russe.

- ***Disposition mentale – 3e caractéristique : le triptyque patriotisme–unité–souveraineté***

Les retex étudiés et les retours des auditeurs bénévoles évoquent souvent la chance de disposer en France de ce système de santé d'accès gratuit. En dehors des considérations polémiques liées à l'état actuel et à venir de ce système, l'on doit noter que si l'État est en soutien actif et résolu, « au chevet » de ses hôpitaux, il ne l'est vraisemblablement pas en pro-action et prophylaxie si l'on peut se permettre l'expression. Pour prendre les mots critiques de Karim Lamouri faisant un parallèle dont on sera seul juge : « *Le Campus cyber, c'est un bâtiment. Ça canalise un temps les forces vives. C'est un projet immobilier. Ce n'est pas essentiel. Faire la tournée des hôpitaux et des entreprises de France en quête de leurs besoins et de leurs vulnérabilités, ça c'est essentiel.*[662] » La question est peut-être de savoir si l'État fait ce qu'il peut ou doit pour sauver le système de santé national et ainsi ne pas réduire leur portion congrue aux hôpitaux afin qu'ils puissent davantage se consacrer, dans un cadre plus serein, aux impératifs de sécurité informatique. Notons par ailleurs le rôle patriote *pro bono publico* joué par des hackers bénévoles via les initiatives d'organisations lucratives ou non telles que HWB, Yogosha (programme *Hack4Values*) ou encore YesWeHack.

- ***Dispositif opérationnel – 4e caractéristique : l'information au centre du jeu stratégique***

Si les hôpitaux ne sont pas censés être en concurrence, du moins sont-ils confrontés à des attaques tout à fait préjudiciables. Dans ces établissements, l'information a vocation à circuler le plus aisément possible, mais pour des raisons fonctionnelles. Or, certaines mesures de protection élémentaire et de sensibilisation permettraient de parer au moins aux attaques les plus rudimentaires. D'un point de vue intellectuel, une thèse de doctorat en sciences informatiques et cybersécurité des Mines-Télécom d'Alès nous renseigne sur la grande

[662] Entretien avec l'auteur, 07/07/2023.

indigence de la littérature scientifique s'intéressant à la question de la SSI des centres de soins médicaux[663]. En outre, ce travail témoigne des besoins flagrants en termes de sensibilisation des personnels soignants, « *d'éducation et d'intelligence situationnelle qui doivent être intégrées impérativement*. » Il note dans cette même idée qu'il est impératif de les impliquer à la participation à la cybersécurité (formation externe, inclusion de sous-traitants), « *dans la mesure où ils investissent des ressources et connaissances, qui peuvent ou non être uniquement orientées vers le profit*.[664] »

- ***Dispositif opérationnel – 5e caractéristique : maîtrise de l'information via le triptyque acquisition–sécurité–influence***

Le niveau moyen de cybersécurité des personnels d'entreprises est faible en France selon « Bob », qui travaille à l'ANSSI[665]. Selon lui, ce sont les plus grandes qui suivent les « bonnes pratiques », suivies de quelques rares PME plus sensibilisées que la plupart où les hackers ne sont pas forcément utiles. Pour les plus grandes en revanche, ils le sont vraiment. Dans cette perspective, où placer les hôpitaux ? Si l'on s'en tient à leur degré d'importance et à la nature proprement vitale de leur activité, il va sans dire qu'il est nécessaire de les appréhender tels des grands groupes. Du reste, la taille – ici révélée lors des retex – de leurs parc et réseau informatiques est significatif : plusieurs datacenters pour certains, des centaines de serveurs, des milliers de terminaux fixes et nomades. Au sujet de l'internalisation nécessaire ou potentielle à effectuer dans le domaine de la SSI, Victor Poucheret apporte des précisions intéressantes. D'après lui, « *elle est difficile à réaliser car il n'y a pas de savoir-faire correct en interne, et compte tenu que les meilleurs spécialistes sont d'esprit indépendant. La position du hacker en général, c'est un peu l'image de l'électron libre. Et il faut un esprit d'attaquant, et dans l'actualisation perpétuelle des connaissances qu'il s'agisse des outils, des progrès de la technologie et de la cybermenace. Il vaut mieux que les sous-traitants (hackers) gardent leur indépendance, mais fa*[ssent] *avancer les connaissances des salariés internes* [RSSI et personnels soignants] *pour faire progresser l'organisation selon son cycle de vie*.[666] » Voici donc une très plausible réponse à la question que posent en creux les retex examinés dans notre étude. Des hackers dotés d'un esprit créatif et offensif, toujours en maintien à l'état de l'art de la cybermenace et des TIC constitueraient un atout-clé pour améliorer la sécurité des hôpitaux.

[663] Ahmed Nasir-Baba, *Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience*, thèse de doctorat en sciences informatiques et cybersécurité, Institut des Mines-Télécom (IMT) d'Alès, université de Nîmes, 2022.
[664] Ahmed Nasir-Baba, *idem*, pp. 138-139.
[665] Entretien avec l'auteur, 15/10/2021. Voir aussi Philippe Trouchaud, *La Cybersécurité face au défi de la confiance*, Odile Jacob, 2018, 192 p.
[666] Entretien avec l'auteur, 14/11/2021.

De même, une meilleure communication interne entre des équipes souvent compartimentées assureraient une meilleure coordination.

- ***Dispositif opérationnel – 6e caractéristique : processus réticulaire via un dispositif intelligent***

En effet, les retex sont unanimes quant aux bienfaits engendrés paradoxalement par ces cyberattaques, car elles ont eu le mérite de solidariser les forces vives internes en lien avec des soutiens externes venant en particulier de l'État mais aussi d'acteurs privés. Ce que soulignent par ailleurs les témoignages à propos de l'appui inconditionnel des centres de soins régionaux, à l'image du Centre hospitalier de Dax qui parle d'une solidarité sans faille de ses homologues du Sud-Ouest[667]. Néanmoins, c'est toujours en réaction et non en anticipation que les avantages procurés par la synergie des acteurs sont félicités. **L'expression « *les gars de l'informatique* », pour reprendre la formule souvent usitée par les équipes de personnels soignants, a ceci de caractéristique qu'elle révèle non l'antagonisme, mais l'incommunication et l'incompréhension de deux mondes pourtant complémentaires au sein d'une même entité**. Les informaticiens ont leur jargon, et si les vocations et compétences pédagogiques de ces équipes sont certainement disparates d'un établissement à un autre, elles buttent en tout état de cause souvent sur les aspirations et pratiques quotidiennes des soignants qui, d'une part, ont certes d'autres priorités bien compréhensibles, mais d'autre part la fâcheuse habitude de contourner des mesures de sécurité, perçues plus comme un souci ponctuel récurrent que comme une solution d'anticipation à d'autres problèmes potentiellement incoercibles dans un temps moins immédiat.

Le manque d'homogénéité dans le niveau de sécurité des hôpitaux constitue en soi une difficulté alors que l'ensemble du tissu des hôpitaux devrait être astreint par les autorités étatiques à l'uniformisation de leurs politiques de sécurité. Comme l'indique Victor Poucheret, « *Il y a une jonction, un équilibre à faire entre les ressources internalisées et la collaboration avec des "attaquants" externes*. » Ajoutant ce qui vaut tout autant pour les organisations privées que pour les hôpitaux publics : « *Les entreprises savent qu'il faut se mettre à la page concernant la sécurité informatique et numérique mais elles ne savent pas vraiment ce dont elles ont besoin car la matière est pointue, y compris pour des équipes d'informaticiens classiques. L'IT n'est pas la SSI et encore moins la cybersécurité, mal comprises des dirigeants*.[668] »

[667] https://fr.linkedin.com/posts/adusonchet_retex-cyberattaque-ch-dax-activity-6957346875788136448-CSjj
[668] Entretien avec l'auteur, 14/11/2021.

***Boussole de disposition mentale* :**

1- Posture et intentionnalité

2- Culture et intelligence

3- Patriotisme et souveraineté

4- Organisation et cohésion

***Boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité

6- Méthodes et outils

7- Intégration et synergie

8- Plasticité et agilité

1- Les travaux de thèse précités permettent de saisir le manque de préparation de la plupart des centres de santé. Notamment, il est fait mention du constat d'un manque de développement et d'amélioration de stratégies pour évaluer la cyber-résilience des établissements et leur posture face au risque. Ce qui nous ramène à la nécessité de réaliser des audits poussés et au niveau de l'état de l'art de la cybermenace.

2- Nous avons pointé à travers les retex des établissements le manque de sensibilité et d'acculturation à la sécurité informatique de la part des personnels soignants et directions. Ahmed Nasir-Baba évoquant même la nécessité d'accroître les campagnes de sensibilisation, d'éducation et d'intelligence situationnelle. Autant de recommandations qui s'arriment à une politique de sécurité qui pourrait et devrait être co-construite entre les différentes équipes des hôpitaux, et pas seulement selon une modalité pouvant être perçue comme coercitive car provenant du service informatique.

3- On a évoqué le rôle d'accompagnateur permanent que devrait jouer l'État, et son intérêt à qualifier et proposer des prestataires atypiques pour suppléer les RSSI des hôpitaux. Les profils de hackers seraient ainsi tout indiqués. Les initiatives gracieuses réalisées par des hackers dans des cadres légaux montrent que ceux-ci sont forces de propositions et peuvent être loués quant à leur esprit patriote. Sans nier que *faire savoir son savoir-faire* était l'une des clés de la réussite commerciale des hackers comme de tout prestataire de services et entrepreneur. Les exemples de nations à la posture affirmée d'intelligence économique le démontrent très certainement.

4- Les questionnaires réalisés dans le cadre des travaux de thèse précités nous apportent une nouvelle fois la preuve que la faible conscience du risque cyber est préjudiciable aux centres de santé[669]. La cohésion des équipes n'apparaît qu'en situation de crise là

[669] Voir annexe 2.

où elle devrait être permanente, comme le révèlent avec clarté les retex. L'organisation des hôpitaux devrait s'adosser à une logique de *security by design* avec un focus sur la sécurité physique, presque toujours inexistante. Les impacts inventoriés sont de plusieurs ordres : dégradation des conditions de travail ; disruptions ; destructions ; compromissions et vols de données sensibles médicales. Les préconisations finales de la thèse encouragent : l'amélioration des processus et outils d'évaluation des risques ; le développement de la recherche empirique pour documenter les pratiques de sécurité ainsi que le perfectionnement dans la modélisation des menaces ; l'exploration de scénarii d'attaques créatifs « *car les attaquants évoluent sans cesse* » (avec utilisation progressive de techniques de haut niveau), donc le maintien de suivi des mesures de cyber-résilience/sécurité ; enfin, l'exploration des techniques et outils de *pentesting* (avec tests *in situ* basés sur des scénarii de vie réelle) et le développement du renseignement sur la menace (CTI).

Enfin, plusieurs retex attirent l'attention sur la nécessité d'employer des mesures de sécurité complémentaires qui peuvent grandement limiter les compromissions et mitiger les attaques, comme la multi-authentification/authentification forte/second facteur d'authentification. Le directeur du Centre hospitalier de Corbeil-Essonnes a notamment souligné son importance et le fait qu'elle était peu à peu implémentée dans l'ensemble du SI de l'établissement. On notera par ailleurs et comme anicroche que la plateforme de gestion documentaire de l'hôpital se trouve être la suite *Office 365* de Microsoft, démontrant une nouvelle fois qu'au regard de la confidentialité des données – ici de santé, donc hautement sensibles –, les centres de soins ne faisaient pas exception à la faiblesse nationale en termes de souveraineté numérique.

5- Si l'État a fourni beaucoup d'efforts à la sécurisation de ses hôpitaux, cela reste insuffisant, et son accompagnement doit se faire dans un temps long et non seulement en réaction. En l'espèce, nous avons évoqué l'importance d'homogénéiser les politiques de sécurité informatique de tous les établissements de santé à l'échelle nationale. La transversalité et la mutualisation constatées lors de crises cyber par ces mêmes acteurs ne doit pas constituer l'exception mais la règle. L'apport de prestataires externes, à la plus-value forte, comme on peut l'imaginer avec l'emploi de hackers, éviterait d'empiler les mêmes compétences entre RSSI internes et spécialistes externes non de l'attaque mais de la défense des SI.

6- De fait, le croisement des méthodes des hackers avec celles de « défenseurs » plus classiques s'avèrerait des plus efficace dans la sécurisation des centres médicaux. Cette mutualisation des états d'esprit et des pratiques serait un plus indéniable. Par conséquent, le travail des *pentesters* viendrait opportunément renforcer cette

sécurité, comme en attestent les résultats fournis par Ahmed Nasir-Baba dans sa thèse. En effet, dans ce cadre il a soumis à des attaques informatiques les dispositifs nomades utilisés dans les hôpitaux et en a tiré les constats suivants : les tests d'intrusion réalisés se sont avérés tous concluants et démontrent la faiblesse desdits systèmes, en particulier sur la sécurité des réseaux et accès WiFi[670]. Plusieurs techniques ont été utilisées à cette fin : injections de code malveillant (RCE, SQLi[671]), manipulation de données (ex : codes barre), exfiltration de données via des *remote administration tools* (RAT), ou encore attaques DOS (*denial of service*).

7- On l'a dit, la synergie n'est possible que si chaque acteur comprend l'intérêt du rôle de l'autre. Cela nécessite une ouverture croisée entre le savoir technique et la mission contraignante mais obligée des uns (informaticiens, RSSI) et le métier et la mission d'intérêt sanitaire des autres (personnels médicaux). C'est de ce dialogue et de cette empathie réciproque que viendra la solution pour assurer une plus grande anticipation à la menace.

8- Les personnels soignants font très souvent preuve d'un sens de l'adaptation dans le cadre de leur métier, mais sont moins à même de se conformer aux règles de sécurité qui pourtant peuvent leur assurer, une fois comprises et « vécues », une marge de manœuvre insoupçonnée. À l'image de la loi qui en réalité émancipe, les mesures sécuritaires peuvent permettre aux personnels soignants de saisir l'opportunité d'une forme de liberté dans leur activité quotidienne. Surtout, s'éviter au mieux ou mitiger au pire la « tempête » et le « cyclone » décrits avec justesse par les équipes du Centre hospitalier de Dax.

## Caractéristiques-clés – synthèse et hypothèses

Quels enseignements tirer de ce cas à partir des caractéristiques-clés, et ce dernier répond-il à nos hypothèses de recherche ?

• L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)

• L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)

[670] Voir annexe 2. Ahmed Nasir-Baba, *Cybersecurity in Healthcare System*, *op. cit.*, pp. 117-118 ; 138-139.
[671] *Remote code exécution* (RCE), injection SQL (SQLi). Ahmed Nasir-Baba, *ibid.*, pp. 117-118.

• L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

### Synthèse :

Cette étude de cas nous a permis de dégager des éléments d'informations éclairants quant à la problématique de cybersécurité des centres de santé :

- **D'abord, le constat d'un manque d'acculturation flagrant des équipes de personnels soignants et le positionnement insuffisant des autorités pour harmoniser et accompagner la maturation sécuritaire des établissements médicaux. Par ailleurs, la faiblesse des budgets alloués à l'informatique en général et la sécurité en particulier démotive les RSSI**. Autre point : l'absence de ligne stratégique et d'uniformité dans les politiques de sécurité des établissements, acteurs collectifs d'un système de santé unique qui pèche pourtant par son manque de coordination. En effet, les hôpitaux gèrent le plus souvent ces aspects de manière autonome et hétérogène.

- Ensuite, le besoin exprimé et pourtant non satisfait d'emploi de prestataires extérieurs dotés d'une approche innovante ou à rebours des spécialistes classiques de la sécurité numérique. Il est question bien sûr des profils de hackers, qui ne sont jamais vraiment mentionnés dans les retex (par méconnaissance ou par préjugés négatifs à leur encontre ?), lesquels pointent pourtant tout naturellement vers les *chapeaux blancs*.

- Enfin, on relève un manque de synergie évident entre les différentes parties prenantes du bon fonctionnement des hôpitaux. Ces derniers expriment pourtant leur contentement voire leur plaisir d'avoir pu mutualiser toutes les forces vives internes et externes mais *a posteriori*, seulement dans les séquences de gestion de crise. Après ces incidents de sécurité somme toute récents, il faut toutefois noter que ces crises ont le mérite de faire intégrer les enjeux cyber. Gageons qu'elles permettent à l'avenir d'infuser une véritable culture de cybersécurité.

Ces constats généraux font écho à la réflexion préalable posée par Christian Bourret, dans laquelle il préconise d'associer plus étroitement l'ensemble des acteurs publics et privés des

territoires, en favorisant l'action de la gendarmerie pour une approche globale de sécurité économique et de cybersécurité[672].

### Rappel des hypothèses :

1 – ces trois mondes (hackers–État–entreprises) sont intégrés et dans une co-construction (interaction et communication décloisonnées, projets communs, logique de dispositifs intelligents, synergie…)

2 – ces trois mondes sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas (incommunication) par manque de synergie

3 – ces trois mondes s'ignorent (acommunication)

Le cas ici étudié nous permet d'avancer que deux de ces trois mondes sont en interaction mais plutôt en cas de situation de crise après un incident de sécurité. De ce fait, ils ne s'ignorent pas, voire communiquent avec fluidité. Ces deux mondes sont les autorités étatiques (ANSSI, ARS…) et les entreprises spécialisées qui assurent les remédiations. Néanmoins, les hackers sont quasiment absents hormis dans le cadre de leurs actions *pro bono publico*, mais très rarement – en anticipation – à la demande des centres de santé eux-mêmes. Les prestataires de sécurité informatique sollicités en plus des RSSI internes ne peuvent que rarement être assimilables à des hackers éthiques. Nous pensons qu'il est raisonnable de ne valider aucune hypothèse ou bien de se placer entre l'hypothèse n°1 et l'hypothèse n°2.

* * *

### Résumé de l'étude de cas :

Ce troisième cas portait, quant à lui, sur les cyberattaques régulièrement subies par les centres hospitaliers français. **Deux enseignements focaux ont été retenus : d'abord, que les établissements de santé manquent de ressources financières et qu'à l'image des autres institutions publiques et dans une certaine mesure privées, la part de leur budget alloué aux SI et plus encore à leur sécurité était négligeable ; ensuite, que pour des raisons compréhensibles mais dans le même temps synonymes de grande vulnérabilité, les personnels soignants manquent d'une**

[672] Christian Bourret, « Pistes de réflexions sur les actions et les potentialités de la Gendarmerie nationale. Le cas du Couserans dans le département de l'Ariège (Pyrénées) », *Cahiers de la sécurité et de la justice*, 2022/3 (N°56), pp. 44-51.

**culture de sécurité, ce qui induit une surface d'attaque élargie ouverte à la cybermenace**. Cette cybercriminalité charognarde faisant montre d'un opportunisme aigu, les hôpitaux deviennent des proies évidentes. En l'absence de hackers dans ce contexte, mais du fait des besoins orientés vers ce genre de profils et des réactions synergiques en réponse aux crises, nous avons donc embrassé les hypothèses n°1 & 2.

**Figure 41 :** *Tableau récapitulatif de l'étude de cas n°3*

| ***Boussole de disposition mentale :*** | **Bilan ±** |
|---|---|
| 1- Posture et intentionnalité | • Manque de préparation face aux attaques<br>• Pas d'audits en amont pour évaluer le risque cyber au mieux, la cyber-résilience au pire |
| 2- Culture et intelligence | • Manque d'acculturation…<br>• et de sensibilisation/éducation au risque cyber |
| 3- Patriotisme et souveraineté | • Posture d'intelligence économique faible<br>• Traitement (considération ?) par l'État des établissements hospitaliers comme services publics faible<br>• Pas d'accompagnement d'initiatives pourtant bénévoles de certains hackers au chevet des hôpitaux |
| 4- Organisation et cohésion | • Cohésion d'équipe face au risque cyber ponctuelle car conditionnée aux attaques subies<br>• Satisfaction collective après la mutualisation des moyens, compétences et dynamisme, mais lors de crises cyber<br>• Sécurité physique également faible au-delà des aspects informatiques |
| ***Boussole du dispositif opérationnel :*** | **Bilan ±** |
| 5- Adaptabilité et transversalité | • Réactivité mais non proactivité de l'État face aux cyberattaques contre les hôpitaux<br>• Mutualisation des forces ponctuelle et non continuelle chez ces derniers |
| 6- Méthodes et outils | • Compétences axées sur la défense donc manque d'anticipation des RSSI des centres de santé face aux pirates<br>• Faiblesse générale des établissements en termes de sécurité informatique |
| 7- Intégration et synergie | • Manque de compréhension mutuelle de chaque métier<br>• Manque de dialogue avec et d'intérêt porté aux équipes d'informatique |
| 8- Plasticité et agilité | • Inadaptation des personnels soignants aux mesures et règles de sécurité<br>• Mais prise de conscience de ce problème pendant et après une crise/attaque |

### 4) Le cas Florent Curtet : parangon des rapports ambigus entre hackers et autorités

« *Obéir, c'est trahir ; désobéir c'est servir*.[673] »

Très peu médiatisé à l'origine (un entrefilet anonymisé dans un organe de presse nationale[674]), ce cas est documenté sur la base des Mémoires publiés par Florent Curtet et de témoignages recueillis auprès de protagonistes de l'affaire. Ce corpus est par ailleurs enrichi par des entretiens d'autres hackers ou de membres des forces de sécurité. Ce cas est exceptionnel en France et révèle une partie des dessous de la relation que peuvent entretenir ces profils avec les autorités.

Né en 1989, Florent Curtet n'est pas un *digital native* tel qu'on désigne ces jeunes de la « génération Z » située entre 1997 et 2010. Il n'est pas né « dans les écrans », mais plutôt avec eux. Il fait ainsi partie de ce que la *Harvard Business Review* a qualifié de génération des *Milléniaux* issus des années 1984-1996. Cette décennie a vu l'introduction de l'informatique grand public dans les foyers ainsi que l'émergence de l'Internet. Depuis le *phreaking* des années 1960 puis les cartes téléphoniques détournées dans les années 1990, la « bidouille » sur les dispositifs électroniques s'est déployée à l'échelle des réseaux informatiques transnationaux.

C'est à cette époque que la cybercriminalité apparaît et se développe, sur des forums web ou des réseaux IRC (*Internet Relay Chat)*[675], l'ancêtre des messageries de discussions synchrones. C'est l'âge d'or des magazines papier sur le hacking dans le sillage des célèbres *Cult of the Dead Cow* et *Phrack*[676], à la fois journaux et associations hacktivistes nés au milieu des années 1980. En France notamment, la communauté *Hackerz Voice*, avec sa revue *Hackademy Magazine* et son « école » *The Hackademy*, fait parler d'elle en 2002 lorsque ses « profs » et rédacteurs sont placés en garde à vue pour avoir annoncé l'identification de nombreuses failles sur les sites web de plusieurs banques nationales[677].

[673] Slogan de la Résistance française. Cité par Florent Curtet en exergue de son ouvrage.
[674] Entretien avec Florent Curtet, 30/09/2021. Pour sa première arrestation. Aucune couverture médiatique pour la seconde en 2022.
[675] IRC est un protocole de communication formalisé par les RFC 1459, 2810 et 2813. Les clients IRC ont été progressivement remplacés dès la fin des années 1990 par des messageries instantanées propriétaires comme en premier lieu MSN Messenger. La plupart des messageries synchrones actuelles sont basées sur le protocole IRC.
[676] https://cultdeadcow.com/ ; http://phrack.org/
[677] https://www.lemonde.fr/archives/article/2002/09/30/garde-a-vue-pour-les-dirigeants-de-hackerz-voice_292460_1819218.html, consulté le 10 mai 2023. La communauté *Hackerz Voice* a accouché en 2003 de la grand-messe annuelle *La Nuit du Hack*, rebaptisée *Le Hack* en 2018. Voir https://hzv.fr/, consulté le 17 avril 2023.

C'est dans cette « culture du hack » qu'a baigné Florent Curtet depuis ses plus jeunes années. De son premier contact fulgurant avec les ordinateurs, le jeune francilien va développer une passion sans bornes pour l'informatique jusqu'à en maîtriser les rouages pour finalement les détourner et basculer dans l'illégalité. Son cas n'est pas commun, surtout en France, et son témoignage exceptionnel car on sait très peu de ce lieu interlope communément mais à tort appelé le *Darknet*. Ses Mémoires de trentenaire, Florent Curtet les a intitulés « Hacke-moi si tu peux »[678] dans un clin d'œil manifeste au film de Steven Spielberg mettant en scène un jeune homme jouant des failles administratives et humaines, et se jouant des autorités. Or, le destin des deux protagonistes va se croiser dans une sorte de trajectoire diachronique non dénuée d'ironie. En des époques différentes, en effet, ces deux « génies » de la « bidouille » font montre d'un savoir-faire dont la police notamment voudrait bien disposer. C'est cette expertise, mise plus tard au service du bien, qui montre toute l'ambiguïté des rapports asynchrones entretenus par les autorités avec les hackers. Des rapports rarement connectés, au sens propre comme au figuré.

### a) *De hacker noir…*

Après des années d'échanges et partages sur des sites *underground* et d'apprentissage en autodidacte, à 15 ans Florent Curtet bascule réellement dans la cybercriminalité, fusse à son corps défendant[679]. Ce qui n'avait consisté aux prémices qu'en du détournement mineur de lignes fixes locales et de cartes téléphoniques (*phreaking*), s'était transformé en vols et recels d'identifiants de cartes bleues (*carding*) et leur clonage/reprogrammation (*skimming*). De fil en aiguille, le jeune *black hat* se fait un nom – ou plutôt un pseudo, « Zetun/Theeeel » – dans un *e*-marché parallèle (« DarkMarket ») et pousse le vice jusqu'à contrefaire des billets de banque dont il usera pour se créer une sphère sociale et épater son nouveau cercle d'amis intéressés. Or, les agences américaines ou internationales, FBI, CIA, DEA et Interpol en tête, cherchent à démasquer et démanteler ces réseaux parallèles. Deux ans plus tard, quand le service extérieur américain fait part de ses inquiétudes aux autorités françaises sur ce qu'elle estime être le « cerveau » de la cybercriminalité hexagonale, la police a déjà infiltré les fondations de ce qu'on appellera plus tard le *Darknet*. Parmi ses compères virtuels, « Zetun » compte sans le savoir plusieurs « indics » des renseignements états-uniens et de la police judiciaire, laquelle est en train de monter un coup de filet sur le territoire national. Entre 2007 et 2009, plus de 56 personnes vont être arrêtées, treize dont deux français le seul 12 juin 2007[680]. C'est le procureur de la République de Marseille qui a instruit une procédure sur alerte

[678] Florent Curtet (avec Sophie Garcin), *Hacke-moi si tu peux. Mémoires d'un cyperpirate repenti*, Le cherche midi, 2023, 204 p.
[679] *Hacke-moi* si tu peux, *op. cit.*, p. 52.
[680] *Idem*, pp. 117-132.

de la cellule parisienne de la CIA, puis diligenté l'enquête pilotée par l'OCLCTIC[681] qui aboutira à l'arrestation des administrateurs du forum DarkMarket[682].

### b) *… à hacker blanc : réhabilitation et « réinsertion »*

Comme le note le policier qui a supervisé sa garde à vue, Pierre Penalba, « *le début de l'affaire a été compliqué, parce qu'il ne s'agissait pas du profil criminel type. Juste un jeune gamin qui avait trouvé une faille dans le système pour se faire plaisir, briller et se faire une place socialement, auprès de ses amis notamment. Pas question d'un criminel chevronné.*[683] » Effectivement, Florent Curtet mentionne à plusieurs reprises son besoin de reconnaissance parmi ses pairs virtuels, comme de sociabilité parmi ses camarades du « monde réel ». Adolescents ou adultes, la réputation voire l'égo ainsi que des problèmes d'hyperactivité et de socialisation sont souvent invoqués au sujet des hackers pour expliquer leurs inclination et méfaits. L'un des plus célèbres d'entre eux, l'Américain Kevin Mitnick, arrêté à 35 ans notamment pour avoir piraté le NORAD[684], a un profil sensiblement proche de celui de Florent Curtet.

Après sa mise en liberté conditionnelle, Florent Curtet passe son bac et poursuit des études supérieures dans le commerce. « *Comment devient-on un étudiant normal, docile apprenant, après avoir été souverain de la Toile ?* [685] » Durant ces années, le jeune Florent va démontrer des capacités relationnelles confinant à l'ingénierie sociale, mais légale. Après un bref passage dans une mutuelle comme gestionnaire financier, il renoue avec sa passion de l'informatique en intégrant Mines-Télécom pour devenir ingénieur spécialisé dans l'audit des systèmes d'information (SI). Devenu consultant en SI, il fait ses armes et collabore tour à tour avec des cabinets de conseil pour des clients privés et institutionnels tels que des ministères et des organisations internationales : ONU, Interpol, AIEA[686]. Connu pour son casier judiciaire et passant sous les fourches caudines d'enquêtes de proximité, en tout état de cause procédurales, ce passé ne lui porte pas forcément préjudice. Florent Curtet a décidé de jouer franc jeu. Certains clients privés (entreprises) sont réticents, d'autres non[687]. On le sollicite et le missionne en cas de crise, dans le cadre de réponses à incidents : « *Florent Curtet peut-il*

[681] OCLCTIC : Office central de lutte contre la criminalité liée aux TIC. En 2014, l'OCLCTIC a été intégré dans la Sous-direction de la lutte contre la cybercriminalité.
[682] À son apogée, le forum aura rassemblé 2000 vendeurs et 500 000 utilisateurs de tous pays. Voir *Hacke-moi…*, *op.cit.*, p. 125.
[683] Entretien avec l'auteur, 07/07/2023. Pierre Penalba est alors le chef d'une cellule de lutte contre la cybercriminalité à la PJ de Nice. Son équipe est pionnière au sein de la police française.
[684] Pour *North American Aerospace Defense Command*, Commandement de la défense aérospatiale de l'Amérique du Nord. Kevin Mitnick fut diagnostiqué Asperger (aujourd'hui TSA).
[685] *Hacke-moi…*, *op. cit.*, p. 137.
[686] Entretien avec l'auteur, 30/09/2021.
[687] *Ibid.*, 30/09/2021.

*faire du renseignement sur le Dark Web pour voir si nos données ont été diffusées ?* [688] » mime-t-il. La relation est contractuelle, nécessaire, opportune. Ce passé ne l'a pas desservi, par pragmatisme utilitaire de la part de ses recruteurs constate-t-il[689].

### c) *La collaboration avec les entreprises*

Quand elles ont du moins conscience du risque cyber, les entreprises font de plus en plus appel à des experts en cybersécurité. « *Ça commence à rentrer dans les mœurs. Mais c'est une très très lente prise de conscience. On n'a pas encore les bons réflexes en France pour beaucoup d'entreprises. "On n'est pas des cibles" disent-elles en général.*[690] » Par ailleurs, le qualificatif « utilitariste », pour désigner l'intérêt des entreprises pour les hackers, revient souvent dans les témoignages. « *Le lien avec les entreprises est froid, glacial même* » confie Julien Métayer, « *car les hackers sont soupçonnés d'être à la source du problème qu'ils identifient et font remonter.*[691] » Dans le grand public comme chez les chefs d'entreprises, on commet donc un amalgame, que les médias contribuent d'ailleurs à perpétuer. Le mot « hacker » est, en effet, systématiquement associé à la notion de pirate informatique, même si certains journalistes commencent à marquer le distinguo, pas dans les mots qui restent interchangeables, mais du moins dans la présentation qui est faite de la nature de leurs activités respectives[692]. Fabrice Epelboin confirme les propos de nombre de hackers et signale qu'à de rares exceptions, les entreprises ne les traitent pas bien. *« Le rapport est on ne peut plus utilitaire. Elles ne bâtissent pas grand-chose. Les hackers en sont bien conscients mais jouent le jeu car ils sont très demandés.*[693] » Yassir Kazar, cofondateur de Yogosha, renchérit mais temporise : « *Ces relations sont certes utilitaristes, mais c'est global, c'est le marché : Yogosha crée un marché pour les hackers.*[694] » Par ailleurs, Victor Poucheret fait remarquer que les entreprises les plus impliquées contractent parfois un suivi sur du long-terme : trois, cinq, jusqu'à dix ans. Dès lors, l'engagement se cristallise sur un haut niveau de confidentialité et une confiance certaine. « *Il y a de l'occasionnel comme du plus impliqué. Les rapports hackers-entreprises dépendent du niveau de sensibilisation, et donc du degré de maturité, qui a crû depuis les grandes cyberattaques de 2017 et la crise du Covid avec le télétravail accru. Donc les entreprises cherchent de l'expertise sur l'offensive. En revanche : on n'est pas dans une approche globale de la sécurité.* »

[688] Entretien avec Florent Curtet, 30/09/2021.
[689] Entretien avec l'auteur, 30/09/2021.
[690] Entretien avec Pierre Penalba, 07/07/2023.
[691] Entretien avec l'auteur, 30/03/2022. Plusieurs autres témoignages vont dans ce sens.
[692] Entretien avec Fabrice Epelboin, 08/04/2022.
[693] *Ibid*., 08/04/2022.
[694] Entretien avec l'auteur, 25/05/2022.

En 2016, sans être clairement établi, le statut de « hacker éthique » voit indirectement le jour en France. C'est dans ce sillon que s'insèrent des plateformes comme Yogosha ou YesWeHack. Typique du hacking éthique, le *pentesting* est l'activité la plus médiatisée. Elle consiste à s'introduire dans les systèmes et réseaux d'une entité en reportant de manière exhaustive toutes les vulnérabilités qui l'ont permis. Florent Curtet est alors recruté par un prestigieux cabinet d'audit multinational et découvre un métier qui n'en était pas un quand il grenouillait dans la flibuste informatique : « *La même chose qu'auraient faite les hackers nocifs, sauf que là, nous étions payés par le patron.* [...] *un jeu d'enfants dans un monde d'adultes.*[695] » Mais le tableau cesse d'être idyllique dès lors que l'on sort de ce *hackerspace* privé et qu'il s'agit d'intervenir chez les clients. Travaillant tour à tour pour des grands comptes de l'aéronautique ou de l'énergie, Florent Curtet évoque cette réalité paradoxale : les cabinets de consulting comme le sien ne travaillent pas forcément au total bénéfice de leurs clients : « *votre manager vous demande d'édulcorer le rapport de test d'intrusion* » s'il s'avère préjudiciable aux clients, sous peine de les perdre. En effet, si leurs équipes informatiques internes laissent des failles critiques de sécurité, ils seront réprimandés par leur direction et risquent bien de ne plus faire appel aux services du prestataire[696].

Après la pandémie du Covid-19, comme beaucoup de hackers autodidactes, Florent Curtet crée sa propre entreprise et apporte aussi son aide bénévole à celles, alors toujours plus nombreuses, qui sont victimes d'attaques par rançongiciel. Partant *a priori* d'un bon sentiment et de son propre chef, il se donne pour mission de jouer les entremetteurs entre lesdites victimes et leurs « cybertortionnaires ». Il s'appuie ainsi sur les réseaux dans lesquels il a évolué naguère et les réactive pour négocier avec les cybercriminels, surtout originaires des pays d'Europe de l'Est. Son but est de jouer « *un rôle d'intermédiation et de temporisation* » dit-il, en essayant de les amadouer[697]. Il dit user tout bonnement d'ingénierie sociale, en jouant sur l'empathie de ces derniers. « *Ces cybercriminels ne sont pas tout noir, ils sont pauvres avant tout. Ils ont un peu d'éthique, dans leur connerie.*[698] » Avant, ils auraient diffusé tout sur le *Dark Web* et auraient bloqué les entreprises (avec impact fort, jusqu'à liquidation). Désormais, il empêche ou minimise des *leaks* de données car il réussit à se faire respecter d'eux, et ils le consultent d'abord. Ainsi, cela limite l'impact sur les victimes, qui ne restent pas paralysées ou ont au moins le temps de se retourner, en sauvegardant les données les plus critiques par exemple. Toutefois, ses activités inquiètent en haut lieu. Ici se révèle toute l'ambiguïté des rapports entre le hacker qu'il est et les autorités qui peinent à appréhender cet électron libre.

[695] *Hacke-moi…*, *op. cit.*, pp. 160, 162.
[696] *Hacke-moi…*, *ibid.*, pp. 160-161, et entretien avec l'auteur, 30/09/2021.
[697] Entretien avec l'auteur, 30/09/2021.
[698] *Idem*.

### d) *Les rapports avec les autorités étatiques*

En parallèle de sa réhabilitation dans le monde privé, Florent Curtet est également sollicité par l'État, ministère de la Défense en tête, au sein d'un « commando informatique » en charge de mettre un terme au scandale du logiciel de gestion des paiements Louvois[699]. Par la suite, plusieurs opérateurs d'importance vitale (OIV) font appel à ses services. Ces organismes privés ou publics sont caractérisés par l'État depuis 2006[700] ; il s'agissait à l'époque de répondre aux risques d'ordre terroriste sur les (infra)structures jugées critiques et essentielles au fonctionnement socioéconomique du pays voire à la survie de la nation. Près de deux cent cinquante ont été désignés en France à ce jour[701]. Comme le note Florent Curtet, les OIV « *ne savent aujourd'hui se passer des services des hackers éthiques.*[702] » On note ainsi une certaine prise de conscience de la part des autorités de l'État pour protéger ces acteurs vitaux.

Mais c'est dans la contribution bénévole que s'illustre surtout Florent Curtet. En effet, issues d'abord très largement de la cybercriminalité, les données qu'il acquiert touchent de plus en plus à des sujets politiques et donc de cyberdéfense, pour lesquels il va se passionner. Tour à tour en 2021, il contacte des ministres ou des représentants du gouvernement : Gérald Darmanin, Bruno Lemaire, Gabriel Attal… dont il a obtenu les contacts grâce aux fuites de données issues du scandale Pegasus[703]. En janvier 2022, par suite d'une cyberattaque qui a touché le CICR, il cofonde l'ONG Hackers Without Borders (HWB) avec Karim Lamouri et Clément Domingo, hackers ou spécialistes de cybersécurité. Sur ces entrefaites, Florent Curtet partage ses trouvailles avec le policier qui l'avait arrêté en 2007. Assez méfiant au début, ce dernier se lie progressivement d'amitié et le soutient tel un mentor : il le fait recruter par son service à la PJ de Nice pour lequel il va travailler gracieusement, faute de mieux. Pierre Penalba précise les modalités concernant ces profils singuliers et très rares : « *Deux méthodes : soit c'est la case justice, soit on essaie de le recruter. On cherche le moyen de l'exploiter car il a une place ultra-privilégiée en termes d'accès à des informations-clés et difficiles à obtenir. En effet, c'est un profil particulier car connu et reconnu des autres hackers, donc il a accès à des*

[699] Le dysfonctionnement de ce système de paiement des soldes sera constaté pendant près de dix ans, de 2011 à 2021.
[700] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000634536. Intégré dans le Code de la Défense en 2007 et renforcé par la LPM 2014-2019, le décret a été doublé de la directive européenne NIS portant le deuxième concept d'opérateurs de services essentiels (OSE) et sera complété par la directive à venir NIS2, associée à une troisième notion « d'entités critiques ». Voir par exemple le blog du juriste et RSSI Marc-Antoine Ledieu : https://technique-et-droit-du-numerique.fr/oiv-ose-critical-entities-projet-directive-ue-decembre-2020/
[701] https://www.sgdsn.gouv.fr/publications/la-securite-des-activites-dimportance-vitale
[702] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 160.
[703] Entretien avec l'auteur, 30/09/2021, et *Hacke-moi…*, *ibid.*, p. 175.

*informations de première main*.[704] » Il agit donc bénévolement mais est tout de même déclaré comme « indic ». Or, le statut « d'indic informatique » n'est pas reconnu par l'administration.

Fin 2021, Florent Curtet fait part à Pierre Penalba de son souhait de servir auprès de la DGSI qui, depuis plusieurs années, lance des campagnes de recrutement pour étoffer ses moyens de cybersécurité. Pierre Penalba prend langue avec le service de renseignement et conseille à son protégé de postuler à une offre d'emploi publique comme opérateur en cybersécurité. Mais le recrutement ne va pas prendre cette forme officielle comme le précise Florent Curtet. On note dans les échanges téléphoniques narrés par ce dernier que les officiers de la DGSI ont hésité quant au statut à lui donner ; ils lui proposent finalement de collaborer ponctuellement en passant « *via un autre type de recrutement, un recrutement parallèle sans que vous apparaissiez officiellement dans les effectifs*.[705] » Selon lui, c'est dû à son passé judiciaire, que sa place n'était pas celle d'un analyste dans un bureau de la DGSI, mais comme agent de terrain numérique, source officieuse, dans l'ombre[706]. De ses mots mêmes, Florent Curtet devient un « honorable correspondant[707] », terminologie usitée du jargon du renseignement. Le hacking et l'infiltration, c'est la deuxième étape confie Pierre Penalba. C'est à celle-là que voulait se hisser Florent Curtet. Il est donc passé à cette phase et a été rémunéré. La DGSI le paie alors en matériel informatique ou en argent cash : « *Tu peux faire ta liste au Père Noël* […] *mais il n'y aura pas de contrat*.[708] » Dès lors, Florent Curtet infiltre les *ransomgangs* et autres forums interlopes pour être véritablement adoubé par la DGSI : il est autorisé à pirater des systèmes informatiques mais doit impérativement tout consigner, pour sa propre protection. Les correspondances avec le service se font par la messagerie instantanée et chiffrée *Signal*.

En 2022, il négocie pour le compte d'un cabinet d'avocats victime des cybercriminels du groupe « Everest ». Pendant ce temps et sans le savoir, Florent Curtet est sous le coup d'une enquête judiciaire montée par une magistrate. En effet, selon Pierre Penalba : « *à un moment, il y a des collègues et une procureure voulant faire du chiffre* (sic) *qui ont voulu lui tendre un piège. Les collègues en question,* dit-il*, c'est l'OCLCTIC et une unité spécialisée de la police de Lyon. Pour la procureure, c'est politique. Ça lui permettrait une promotion*.[709] » Peu à peu, on lui fait savoir qu'il doit arrêter ses intermédiations « contre nature ». Il livre pourtant des informations utiles à l'ANSSI, aux CERTs, à la DGSI et toujours à l'équipe niçoise de Pierre Penalba. En août 2021, comme pour le prévenir de l'imminence de l'inéluctable, un officier de

[704] Entretien avec l'auteur, 07/07/2023 ; *Hacke-moi…*, *ibid.*, p. 180. Pierre Penalba est en 2023 fraichement retraité de la police où il a dirigé un groupe pionnier dans la lutte contre la cybercriminalité.
[705] Florent Curtet, *Hacke-moi*, *op. cit*., p. 184-187.
[706] Entretien avec l'auteur, 30/09/2021.
[707] Entretien avec l'auteur, *idem*. Expression utilisée également par Pierre Penalba lors de notre entretien.
[708] Florent Curtet, *Hacke-moi…, op. cit.*, p. 186.
[709] Entretien avec l'auteur, 07/07/2023.

la DGSI l'appelle spontanément en outrepassant ses attributions. D'abord, il est prié de stopper ses activités d'intermédiation entre les groupes cybercriminels et leurs victimes ; ensuite, le service va couper tout contact avec lui sans le prévenir. Enfin, on lui dit qu'il peut « aller voir à l'Est » et s'enquérir auprès de la DGSE[710]. L'enquête judiciaire à son encontre étant instruite, il est arrêté un an plus tard.

### e) *Clé de lecture du cas d'étude*

Le cas Florent Curtet est intéressant à plus d'un titre. Il nous renseigne sur la manière dont les entreprises mais surtout les autorités (SR, police) établissent des contacts et collaborent ponctuellement avec ce genre de profils particuliers que sont les hackers. En outre, il permet d'appréhender les difficultés formelles (administratives, organisationnelles) qu'éprouvent ces services pour les recruter. Enfin, il est instructif quant à la nature superficielle et utilitariste des rapports qu'ils entretiennent avec eux. En effet, on peut constater qu'il semble improbable que de cette collaboration puisse naître tout projet concret qui pourrait s'avérer constructif d'un point de vue de la cybersécurité nationale. Pour rappel, nous parlons bien d'un hacker, au sens où nous l'avons défini et caractérisé dans la première partie de ce travail. Comme indiqué précédemment, nous avons pris le parti d'assouplir et d'adapter au besoin notre grille théorique pour répondre au mieux à l'analyse du cas. Notamment, nous avons regroupé les caractéristiques 4 et 5.

- ***Disposition mentale – 1ère caractéristique : la complexité du réel***

Que peut nous enseigner l'intelligence économique face à ce cas ? En premier lieu, la question de l'adaptation cognitive des autorités étatiques à appréhender les mouvements browniens de l'environnement globalisé, dont l'instabilité permanente nécessite de penser la complexité. Le cyber induit une augmentation des réseaux communicationnels et des flux informationnels qui perturbent les socles mentaux d'acteurs organisés en administrations verticales. Ceux-ci sont-ils sortis d'une approche cybernétique de l'information, fondée sur l'idée qu'on doit accumuler celle-ci de manière mécanique afin de dissiper le « brouillard de la (cyber)guerre » ? À en juger par les rapports qu'ils ont entretenus avec Florent Curtet, on pourrait en douter. Comme le dit ce dernier : « *J'étais une "donneuse". Je n'ai jamais eu de retours sur les interventions a posteriori des signalements que je faisais. Il y a ce côté frustrant de ne pas pouvoir connaitre la suite.*[711] » Ainsi, la collaboration est en réalité unilatérale et unidirectionnelle. Sans information complémentaire, bien sûr, il est difficile de

[710] Comme l'indique Florent Curtet, « l'Est » désigne la DGSE, sise au 20 bvd Mortier ; « l'Ouest », c'est la DGSI, sise à Levallois-Perret.
[711] Entretien avec l'auteur, 30/09/2021. Voir aussi *Hacke-moi…*, *op. cit.*, p. 190.

juger de l'utilité et de l'opérationnalisation de ces informations acquises notamment par la DGSI. On peut toutefois avancer que, sans échange et avec une communication décousue, il doit être difficile de générer des connaissances actionnables, autrement dit produire de l'intelligence dans le sens où l'entend l'IE.

En tant que « hub humain », Florent Curtet est placé aux intersections de deux mondes comme il l'explique simplement : « *Je parle deux langues, celle de l'entreprise et celle des hackers*.[712] » Il joue d'une logique de relation-interface agile quand il intercède auprès des cybercriminels, que de rares personnes en France connaissent aussi bien que lui. Le témoignage de Guillaume Poupard est intéressant dans cette perspective : « *C'est vrai, il n'y a pas de liens directs hackers-État mais des informations, des résultats transmis, comme avec le cas Florent Curtet. Il est intéressant de ce point de vue. Mais côté parquet/Justice, ils ne sont pas contents.* » En tant qu'ancien maillon de la chaine criminelle, Florent Curtet est bien placé pour savoir que les impératifs moraux, administratifs ou juridiques ne sont pas les référentiels de ces cybercriminels. Ainsi, il est sans doute difficile pour les autorités d'avoir une image claire face à des acteurs particulièrement agiles, quand avoir le *mindset* d'un hacker à l'inverse défloute cette image. Comment expliquer notamment l'incapacité de la Justice et de l'administration policière à concevoir la notion « d'indic numérique » ? Pierre Penalba nous éclaire : « *Il était déclaré en tant qu'indic. Normalement, on peut rémunérer les indics mais la procédure est compliquée et pas du tout dans un cas normal pour le cyber. Donc un indic dans le cyber c'est très neuf, et de fait il n'y a pas de procédure spécifique, d'où la plus grande difficulté encore qu'en temps normal.*[713] »

- ***Disposition mentale – 2e caractéristique : culture de l'intelligence rusée***

Comme le mentionne Pierre Penalba, les policiers comme lui infiltrent des réseaux cybercriminels et s'impliquent parfois au point d'utiliser des armes numériques (*malwares*) pour les démasquer. Mais aussi, bien souvent, d'annuler ces opérations en vertu de garde-fous légaux. « *Sur ces affaires d'infiltration, on travaille comme les services de renseignement : sous légende/anonymat, et on infiltre les milieux du darknet. On est hacker, on ne fait pas semblant de l'être. Ça se repère vite. On nous demande de faire nos preuves, et ça passe par des choses illégales. Il faut montrer patte blanche. Bien sûr, là le risque est trop grand et on*

[712] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 193.
[713] Entretien avec l'auteur, 07/07/2023.

*joue avec la limite, puisque c'est illégal. Donc certains outrepassent mais pas la police, seulement certaines branches de la DGSE, surtout, et de la DGSI.*[714] »

La culture de la ruse, les services spécialisés ou les corps de sécurité l'ont bien sûr. Mais outre que la législation mette logiquement des freins à ce qui leur est possible de faire, ils ne peuvent se passer de profils tel celui de Florent Curtet. « *Ce que l'on fait dans la police,* précise Pierre Penalba, *c'est qu'on essaie de retourner les gens qu'on arrête. On utilise la menace judiciaire et financière. Même avec toutes les ressources du monde et les meilleurs profils, on ne pourrait rien sans l'infiltration et les infos qu'on peut en tirer. Les « gris » sont la bonne interface, comme Florent. Il faut des indics.*[715] » L'art de la manipulation est leur arme. C'est ce qui a toujours caractérisé Florent Curtet. Son témoignage montre combien il a joué de ses capacités relationnelles à de nombreux égards. Il est question bien sûr de personnalité, mais aussi d'apprentissage auprès de réseaux criminels où la duperie est le nerf des interactions sociales, à l'instar du renseignement humain. Or, l'ingénierie sociale est l'une des caractéristiques et parmi les avantages comparatifs des hackers, notamment par rapport aux experts en SSI classiques, dont les audits sont centrés sur les aspects défensifs. De leur côté, les hackers éthiques incluent systématiquement des tests d'intrusion physique (sur site) en plus de leurs tentatives de pénétration informatique. Avec l'appui des directions d'entreprises en général, ils se font passer pour des visiteurs externes et usent d'artifices pour se fondre dans le décor[716]. « *L'ingénierie sociale, c'est le pivot entre les trois sphères* [État-entreprises-hackers]. *On ne hacke qu'en faisant de l'ingénierie sociale* » avance Damien Cazenave[717]. Ce que confirme le lieutenant-colonel de gendarmerie Laurent Leberon : « *Il y a une communauté de pratiques entre renseignement, intelligence économique, voire avec les hacktivistes, mais pas avec les mêmes résultats. Le pivot, c'est l'ingénierie sociale*. […] *Un pivot est en train de se créer autour de l'ingénierie sociale.* » Quand, de son côté, Alexandre Oda pense que c'est, avec la technicité en rétro-ingénierie, la qualité la plus puissante qui valorise les hackers, concluant : « *Ça donne de la lumière aux hackers.*[718] »

[714] Entretien avec l'auteur, 07/07/2023. Il évoque notamment la fois où des cybercriminels lui ont enjoint de pirater un département du ministère de l'Économie (que ces derniers avaient pénétré) pour juger de ses compétences et évaluer le niveau de confiance qui pouvait lui être attribué.
[715] Entretien avec l'auteur, 07/07/2023.
[716] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 163. Voir aussi le documentaire édifiant de Matteo Born, *Hackers : l'intimité violée*, Arte, 2023, 53mn (https://www.arte.tv/fr/videos/112847-000-A/hackers-l-intimite-violee/)
[717] Entretien avec l'auteur, 24/07/2017. Ancien RSSI chez Cdiscount et *venteprivee.com* (actuellement chez Carrefour), ce dernier a organisé de véritables campagnes d'ingénierie sociale (*phishing, vishing* – voie téléphonique) et notamment des tests d'intrusion physique par l'intermédiaire de commerciaux internes. Nous y reviendrons en 3e partie.
[718] Entretien avec l'auteur, 09/07/2020 et 16/06/2021. Une très vaste majorité des personnes avec qui nous nous sommes entretenus souscrivent à cette idée.

- ***Disposition mentale – 3e caractéristique : le triptyque patriotisme–unité–souveraineté***

Il ne serait question de remettre en cause ici le patriotisme des forces de sécurité. C'est précisément une de leurs caractéristiques principales. Il s'agit plutôt d'une observation globale reposant sur les divers témoignages recueillis à propos de la cohérence des missions dont elles sont investies. De fait, d'une manière générale, les forces de l'ordre aimeraient recruter des hackers. Avec des fortunes et intentions diverses, le cas ici analysé atteste cette assertion. Prenons pour exemple la gendarmerie, dont les experts du numérique, les N-TECH, ne cachent pas leur souhait de tisser des liens avec eux. Ils les suivent, les identifient « *mais c'est très encadré juridiquement, ou le serait si on arrivait à trouver des indics dans le milieu* » confie l'adjudant-chef Stéphane Tonelli[719]. Sans parler des moyens alloués : « *Il y a toujours sous-évaluation du politique par rapport aux moyens requis. La conséquence, c'est qu'ici on est juste deux N-TECH pour tout Toulouse !* » Ceci rappelle indubitablement les propos de Pierre Penalba pour la police.

Au-delà de ces aspects administratifs, les difficultés à établir des rapports sains avec ces profils sont flagrantes selon les mots mêmes d'« Alice », hacktiviste de son état : « *Les hackers sont suspects par défaut, et c'est normal quelque part. Mais moi aussi, j'étais en rapport avec les policiers et je doutais tout le temps de leur honnêteté. Je ne savais pas si on essayait de me piéger ou si on pouvait se faire confiance.* […] *On te change de statut.* […] *Alors que ton casier il n'est clairement pas vierge à la base. Certains hackers : gris/hacktivistes, sont sortis de la sphère du hacking parce que c'était dangereux. Les autorités peuvent monter un dossier sur toi pour te charger* » témoigne-t-elle[720]. Le témoignage de Pierre Penalba corrobore ce réflexe conditionné de défiance : « *Tous les profils de hackers sont un peu bizarres. Jamais tout blanc ou noir. C'est une vision binaire qu'on a souvent. On ne peut pas les surveiller 24/24. Il y a un niveau de suspicion permanente notamment pour la police et la gendarmerie.*[721] »

*A priori*, sans confiance toute unité ou solidarité est impossible. Or, si comme le dit Pierre Penalba, les hackers notamment gris représentent la meilleure interface et les meilleures sources, c'est certainement un dilemme cornélien que pose ce genre de collaborations pour les forces de sécurité. Ou pour les hackers eux-mêmes. En effet, au-delà des soupçons d'« Alice », Florent Curtet a, de son côté, vu sa confiance trahie puisqu'il a été arrêté alors qu'il était parallèlement en phase de collaboration avec la DGSI (il continuait de transmettre des informations) et de négociation au bénéfice d'un cabinet juridique. Pierre Penalba indique que des policiers (OCLCTIC/unité lyonnaise) en rapport avec l'enquête menée contre Florent

[719] Entretien avec l'auteur, 28/06/2017.
[720] Entretien avec l'autrice, 01/03/2023. Elle dit avoir subi plusieurs perquisitions à son domicile.
[721] Entretien avec l'auteur, 07/07/2023.

Curtet se sont infiltrés et fait passer pour des avocats de ladite officine. D'après le policier niçois, ces confrères sous couverture ont sollicité l'intercession de Florent Curtet pour ainsi le piéger. Étant donné qu'il l'avait incité à demander une rémunération pour son profil « *de haut niveau* » (sic), Pierre Penalba dit d'ailleurs se sentir un peu fautif quant à son arrestation. Pourtant, la confiance entre les deux hommes est inversement proportionnelle à celle que les différents services de police lui auront globalement témoignée. Cela étant dit, les responsabilités viennent ici de la hiérarchie des unités policières considérées. Pierre Penalba insiste : on a tendu un piège à Florent Curtet dans le cadre d'un coup politique tramé par une magistrate affairiste.

Par ailleurs, il faut noter les rapports de concurrence marqués qui opposent forces de sécurité et services spécialisés. Entre services de renseignement du premier cercle par exemple : selon Florent Curtet, la DGSE et la DGSI ont du mal à coopérer[722]. Tandis que l'ADC Tonelli attribue la création du Centre de lutte contre les criminalités numériques (C3N) de la gendarmerie comme une réponse aux avancées de la police dans le domaine cyber[723]. Saine concurrence ? Pas à en croire Pierre Penalba, fort de ses années d'expérience faites de passages entre la DST/DCRI/DGSI et sa cellule à la PJ de Nice. « *Il y a des tensions entre services, des luttes intestines. C'est une question de politique. Une affaire cyber appelle généralement toujours deux autorités : l'OCLCTIC (police) ou la gendarmerie. Il y a de vrais rapports de force.* » Et de citer plusieurs anecdotes : « *on se jauge et on rabaisse l'autre service, façon cour d'école.* » Il évoque finalement des discussions interservices où la police de Nice était celle qui objectivement maitrisait le mieux le sujet parce que pionnière, et que l'OCLCTIC était en dessous. « *Pendant longtemps, il y a eu dénégation. Aujourd'hui, l'OCLCTIC concède que Nice a le meilleur niveau.* » Pierre Penalba salue du reste la gendarmerie, dont la mentalité est meilleure selon lui, et aussi parce qu'ils savent recruter à l'extérieur de l'institution, notamment des ingénieurs, « *ce que la police ne fait que sur concours. On ne recrute pas des talents. D'ailleurs, la gendarmerie était plus encline à travailler avec Florent Curtet que la police.*[724] »

Enfin, s'agissant du patriotisme, et des ressorts unitaires et solidaires que cela suppose, la plupart des témoignages que nous avons obtenus s'accordent à dire qu'une très grande partie des hackers éthiques et des hacktivistes sont patriotes et l'expriment régulièrement quand ils communiquent. Julien Métayer rappelle que tous ne communiquent pas et que c'est un choix, mais que dès lors qu'il s'agit de se positionner sur les questions techniques de souveraineté numérique en particulier ou de cybersécurité en général, nombreux sont ceux qui affichent

[722] Entretien avec l'auteur, 30/09/2021.
[723] Entretien avec l'auteur, 28/06/2017.
[724] Entretien avec l'auteur, 07/07/2023. Pierre Penalba cite l'ex-chef du COMCYBERGEND, le général Marc Boget.

« leur amour de la patrie » pour reprendre les mots de Victor Poucheret, jeune hacker travaillant dans une entreprise bretonne[725].

> « *On a des ennemis qui sont extrêmement patriotiques, extrêmement nationalistes aujourd'hui. Je pense donc, sans partir sur le débat politique, que la plupart des hackers ont conscience des enjeux cyber et ont l'amour de la patrie. Cette sensibilité, pour moi, elle s'exprime au quotidien, pas sur des sujets de défense étant donné qu'on est indépendants, mais par contre elle s'exprime au quotidien dans le travail qui est fait pour le* pro bono*, vis-à-vis des entreprises, d'ONG, des citoyens qu'on peut aider*.[726] »

C'est dans le même esprit que Florent Curtet s'est engagé en cofondant Hackers Without Borders, en particulier pour des motifs humanitaires et notamment pour alerter les autorités sur la gravité des attaques portées aux hôpitaux hexagonaux. Quant à sonder les raisons profondes de ce patriotisme, on ne saurait s'en tenir qu'aux déclarations des différentes parties, mais faut-il convenir que les actes parlent d'eux-mêmes à travers des projets souvent concrets et des interventions bénévoles au profit d'hôpitaux, d'ONG, etc.

- ***Dispositif opérationnel – 4e et 5e caractéristiques : maîtrise de l'information placée au centre du jeu stratégique***

Compte tenu du niveau d'expertise élevé dont jouit Florent Curtet[727], la question se pose de savoir si ce dernier a été considéré par les autorités comme une pièce maîtresse dans la connaissance d'un milieu par nature mal connu, ou comme un simple pion placé en dehors de tout processus de production d'intelligence. En d'autres termes, sa compétence individuelle s'inscrit-elle dans un creuset collectif facteur de connaissances ? Rappelons à ce titre l'impression d'un manque de sens qui ressort de ses propos. Récupérant de ses odyssées nocturnes dans le *darkweb* des documents confidentiels de l'Armée (tels qu'une carte topographique de la Marine nationale présentant des objectifs opérationnels), des preuves de la préparation de campagnes de phishing et désinformation à l'entame des élections présidentielles ou encore des données compromises liées au gouvernement, Florent Curtet affiche sa déception. « *Mais là non plus, une fois ces éléments transmis à la DGSI, je n'en saurai pas plus*. […] *Le plus frustrant, c'est de ne pas savoir ce qu'il en advient ensuite. Dans le cas de la fuite issue des sites de rencontre, sans doute ont-ils alerté les services de l'Assemblée nationale, du ministère des Affaires étrangères et d'autres encore, mais je n'en saurai pas plus*.[728] » En somme, l'information ne circule pas, tout est siloté. C'est le panoptique

[725] Entretien avec l'auteur, 30/03/2022.
[726] Entretien de Victor Poucheret et Brice Augras, *Thinkerview*, *op. cit*.
[727] Ajoutons à cet égard le fait qu'il ait été notamment contacté par le Département américain de la Défense (DoD) avec qui il a communiqué un certain temps via l'application web sécurisée appelée *Matrix*. Les autorités états-uniennes avaient alors sollicité auprès de l'État français sa protection policière (entretien avec l'auteur).
[728] Florent Curtet, *Hacke-moi*, *op. cit.*, p. 190.

parfait, à moins que ce soit même une relation en « double aveugle », si l'on considère que les services en lien avec Florent Curtet ne s'intéressent qu'aux données brutes que celui-ci leur fournit. Des données qu'on peut qualifier de première main. Mais dont on ne peut juger du traitement effectif ou inexistant et leur inscription dans une stratégie de cybersécurité/cyberdéfense nationale.

Le travail de Florent Curtet s'apparente à une veille active[729] sur les forums spécialisés de hacking et autres marchés noirs numériques. Mais sans informations complémentaires, difficile de savoir si son travail est intégré à celui de la DGSI. Très vraisemblablement est-il considéré comme une source supplémentaire de renseignements semi-ouverts voire fermés eu égard à son aisance à évoluer dans ce milieu. On ne peut faire ici que des suppositions[730]. En revanche, il est à noter la posture pour le moins ambiguë de la DGSI ou de certains services de police, susceptible de créer une dissonance entre leur démarche opérationnelle et leur communication. En effet, Florent Curtet est par exemple autorisé à pirater des SI dans le cadre de leur collaboration mais dans le même temps on se méfie de lui et rompt unilatéralement la collaboration dès lors que le cadre légal « officiel » – la Justice – reprend le dessus. La formule citée par Florent Curtet est assez éclairante, lorsqu'un officier de la DGSI le contacte en catimini pour l'informer que la communication va être rompue et de lui préciser : « *Dès que la Justice passe, on s'efface*.[731] » L'on comprend bien à la fois les interstices laissés par le cadre légal et les ressorts notamment juridiques derrière cette posture policière. Mais alors qu'on interagit avec un ancien hacker noir, il y a comme une incohérence à lui permettre des infractions dans un premier temps pour ensuite et sans coup férir couper le canal et se défausser en raison de considérations légalistes. Certes, les « victimes » de ces intrusions informatiques sont, *a priori*, des criminels. De la même façon, secondant de temps à autre le pôle cybercriminalité de la police de Toulouse, Alexandre Oda évoque des missions que lui aurait confiées ce dernier et qu'il s'est refusé à mener, « *par principe et pour ma réputation* » car il les estimait passablement « *borderline* » (sic)[732].

Du point de vue de la cybersécurité, le travail de Florent Curtet dans le recensement des données gouvernementales qui ont fuité est intéressant, au sens où l'on peut en tirer des enseignements sur l'état de conscience du risque numérique chez nos élites politiques.

[729] Une veille de type CTI/RIC, acronymes/dénominations utilisés par les entreprises privées qui font du « renseignement sur la menace cyber » (CTI en anglais) et par l'État qui fait du « renseignement d'intérêt cyber ».
[730] Notre entretien avec « Christophe » le 03/07/2019, officier de la DGSI en poste à Toulouse, ne donne rien. Il ne souhaite pas se prononcer et élude la question des collaborations avec des hackers. Pourtant, Alexandre Oda mentionne ses liens avec la DGZI de Toulouse et le concours ponctuel qu'il lui apporte ainsi qu'auprès de la police locale.
[731] Florent Curtet, *ibid.*, p. 198.
[732] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.

Notamment, les dangers du BYOD[733] traduits et mis en exergue auprès des autorités lorsque Florent Curtet contacte directement plusieurs ministres après avoir obtenu leur numéro privé. Le jeune hacker rappelle qu'il est de notoriété publique que le chef de l'État préfère utiliser ses appareils grand public personnels plutôt que les téléphones sécurisés *Teorem* mis à disposition par Thalès[734]. Florent Curtet dit avoir été réprimandé par l'ANSSI à la suite de ces remontées d'informations au plus haut sommet de l'État. Or, ce téléphone a été certifié par l'ANSSI, qui en recommande l'usage auprès des instances gouvernementales. Alors que les appareils équipés des systèmes d'exploitation courants tels iOS et Android sont bien entendu particulièrement visés et sources de vulnérabilités, les membres du gouvernement ne tiennent pas compte des préconisations de l'ANSSI. Y peut-elle quelque chose ? En dépit du « hacking protocolaire » des canaux de communication du sommet de l'État, l'ANSSI a-t-elle réaffirmé à l'exécutif la nécessité d'utiliser des SI certifiés (le *Teorem* en l'espèce), ou s'est-elle contentée de condamner l'approche non conventionnelle de Florent Curtet ? Rien d'exceptionnel probablement ici, les gouvernants décidant en dernier lieu. Le témoignage du hacker montre pourtant que l'affaire a fait frémir certains ministres. Les choses ont-elles changé depuis lors ? Il semble que seule l'affaire Pegasus ait véritablement eu un impact, vraisemblablement parce qu'elle a fait l'objet, quant à elle, d'un traitement médiatique considérable. Il s'avèrerait qu'un nouveau téléphone (probablement un *smartphone*, ce que n'est pas le *Teorem*) est en cours d'élaboration[735].

Florent Curtet dit par ailleurs être en contact avec l'ANSSI, laquelle bénéficie pareillement de ses trouvailles tout en ne lui transmettant que de maigres informations en retour. Il précise qu'avec elle le contact est facile et la communication moins opaque, tout en pointant la jalousie et un certain degré d'hermétisme dans les échanges. En particulier, certains fonctionnaires de l'agence lui font remarquer que « *C'est super ce que tu fais, mais tu comprends, à l'ANSSI, on ne comprend pas trop que tu en saches plus que les autres.*[736] ». Il évoque la « *frilosité de l'État* », l'esprit « *bastion* », « *quasi-sectaire* », les « *dogmes* » ou encore la « *fausse politique du secret* » de l'agence. Le travail de Florent Curtet a-t-il finalement exercé une influence ? Sur les autorités françaises, sur les élites politiques, sur les pratiques et la réflexion des services de sécurité ? Il est bien difficile dans le cadre de cette étude et à notre niveau de le savoir.

[733] BYOD (*Bring Your Own Device*), acronyme désignant l'usage dual (personnel/professionnel) des dispositifs numériques. Cette hybridation des usages est préjudiciable à la sécurité des SI.
[734] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 176. Voir par exemple https://www.leparisien.fr/high-tech/qu-est-ce-que-le-teorem-le-telephone-chiffre-que-benalla-a-oublie-de-rendre-16-01-2019-7990023.php
[735] Voir par ex. : https://www.rtl.fr/actu/politique/bientot-un-nouveau-telephone-securise-pour-emmanuel-macron-7900209606
[736] Entretien avec l'auteur, 30/09/2021.

- ***Dispositif opérationnel – 6e caractéristique : processus réticulaire via un dispositif intelligent***

Eu égard aux éléments exposés en amont, il est aisé de considérer qu'il n'y a guère eu de mise en réseau et donc de production réelle d'intelligence dans le cas qui nous occupe. Florent Curtet est affirmatif : il n'y a pas de co-construction avec les autorités et l'État, pas de projet commun, « *chacun reste dans sa sphère*. » Il évoque des contacts limités, des rencontres parfois physiques avec des officiers de la DGSI, « *pour les grands volumes de données, par des baies/disques durs* », mais surtout à distance « *via des NAS*[737] » ou par messagerie chiffrée (*Signal*). Le hacker a fait beaucoup de signalements sous forme d'alertes, pointant des données sensibles de stock ou de flux issues du *darkweb*. Il indique avoir aussi défini des axes de recherche pour aider ses interlocuteurs étatiques. Mais tout « *ça reste du ponctuel, de l'utilitaire* » déplore-t-il et c'est, on l'a dit, unidirectionnel. Florent Curtet évoque par ailleurs les multiples enquêtes de sécurité effectuées par la DGSI à son encontre, le fait qu'on teste sa fiabilité régulièrement. En somme, même si nous nous situons dans l'approche cybernétique de l'information, on peut constater le manque de rétroaction dans la boucle de la communication.

Ce transfert d'informations n'a sans nul doute profité qu'à un acteur, il n'y a eu aucun partage et vraisemblablement aucun apprentissage issu d'un processus d'intelligence collective. Les relations qui ont été entretenues entre Florent Curtet et les différents services étatiques, malgré une communauté de pratiques, n'ont pas permis la création d'un dispositif intelligent. Plusieurs témoignages évoquent la communauté d'intérêt (l'informatique), de pratiques (les outils) et de culture (du renseignement, du hacking parfois) qui peut caractériser certains membres des services de sécurité[738], mais cela ne permet pas de transcender les silos traditionnels administratifs et légaux entre les sphères publique et privée. Julien Métayer confirme : « *L'État et les entreprises ne coconstruisent pas avec les hackers, il n'y a pas de mise en réseau véritable. Et de leur côté, les hackers préfèrent également s'en tenir à ça (d'où leur indépendance), ils préfèrent s'en tenir là car ils ont assez de travail et ne manquent pas d'opportunités dans le contexte de la montée du risque cyber.*[739] » De son côté, Damien Cazenave pointe le manque de réactivité des forces de sécurité et les compétences trop spécifiques dont ils peuvent faire preuve, et finalement le manque d'homogénéité. « *C'est vrai de toutes les autorités étatiques en général.*[740] »

[737] NAS (*network-attached storage*). Entretien avec l'auteur, 30/09/2021.
[738] Entretiens avec Guillaume Poupard (17/04/2023), Julien Métayer (30/03/2022), Christian Harbulot (22/08/2017). Pierre Penalba en est un exemple, Cédric Perrin (ex-DRSD) également (entretien du 05/10/2017).
[739] Entretien avec l'auteur, 30/03/2022.
[740] Entretien avec l'auteur, 24/07/2017.

La question finale du lien social que suppose la mise en réseau de compétences mais surtout d'individus dans une vision commune se pose. Ce lien n'a pas de réalité concrète. L'idée même de dispositifs fermés caractéristiques de services de police ou de renseignement est peu concevable au regard des impératifs de partage, ouverture et synergie propre à un dispositif intelligent. Difficile de concilier un monde ouvert tel que celui des hackers avec celui des autorités et administrations de l'État, alors même que les hackers confirmés ont accès à des informations fermées. Ce lien social est pauvre à en croire Pierre Penalba dont le jugement est sévère :

> « *Il y a clairement un usage utilitariste de leurs compétences. Il n'y a pas d'affect. Avec des niveaux de sensibilité : gendarmerie un peu "humaine", plus que dans la police, et à la DGSI un peu plus qu'à la DGSE. À la DGSI, vous êtes un objet. À la DGSE c'est encore pire : vous êtes jetable. À la DGSE, c'est zéro affect. Ce sont des pions jetables. Dès qu'on n'a plus besoin d'eux, on les lâche*. »

Le sujet des modalités de recrutement est en outre très parlant. Abordant la question, Florent Curtet soutient : « *Les USA sont bien plus matures sur la question de l'intégration entre hackers et autorités publiques. Il y a un gros problème de communication en France. C'est notable dans le recrutement.*[741] » En effet, la NSA américaine, en particulier, monte des campagnes de recrutement via des jeux de pistes « *avec de la stéganographie, de la rétro-ingénierie et tout le reste* » sur son propre site web. « *C'est déjà un premier filtre pour juger de la compétence des candidats.* » Si depuis quelques années des services comme la DGSE organisent ou parrainent des CTF, l'ouverture reste timide en regard de la culture communicationnelle dont font preuve les autorités américaines. Clément Domingo conforte les propos et parle de recrutement « *atypique, alternatif, officieux. Le site web de la NSA, c'est une plateforme de recrutement sous forme de CTF en soi.* [...] *cela requiert des compétences techniques pour trouver les offres d'emploi. À la NSA, il n'y a presque que des hackers, souvent des blacks hats qu'on a choppés*.[742] » Ce dernier note néanmoins des avancées avec l'ANSSI : « *Avec Guillaume Poupard il y a* [eu] *une ouverture avec la communauté des hackers. Même Alain Juillet avait permis une certaine ouverture*.[743] » En revanche, Guillaume Poupard confesse l'échec de ne pas avoir pu changer les méthodes de recrutement sous son mandat, qui demeurent figées sur la « fiche de poste ». « *Je n'ai pas réussi à faire avancer les mentalités et les usages, les garde-fous administratifs, et donc permis le recrutement de*

[741] Entretien avec l'auteur, 30/09/2021.
[742] Entretien avec l'auteur, 15/11/2021.
[743] *Ibid*., 15/11/2021.

*profils atypiques, d'autodidactes. Quant aux profils classiques, type école d'informatique, on sait les recruter mais pas les payer. Certains étaient déçus sur ce point.*[744] »

Du côté de la DGSE, plusieurs témoignages évoquent la figure de Bernard Barbier, ancien chef de la Direction technique de 2006 à 2013. Nous avons justement contacté ce dernier qui, tout en le laissant présumer, a refusé de répondre à la question de savoir si la DGSE recrutait des hackers et comment se passaient leurs relations. Ce n'est certes aujourd'hui plus un secret, et des officiers du service sans étiquette viennent *tamponner*[745] des candidats potentiels notamment à la faveur des grands-messes annuelles du *Hack* et du FIC de Lille ou à l'issue de certaines compétitions comme le CTF404. Recruter ne veut toutefois pas dire intégrer. Concernant la DGSI, l'anecdote contée par « Alice » est édifiante. En 2014, lors d'une phase de recrutement de la DGSE et de la DGSI, on l'a tamponnée en vue d'une mission portant sur une analyse de gros volumes de données. Elle dit avoir été contactée par « *un responsable du bureau des affaires réservées du MININT* » (sic). Sa mission : est-elle en mesure de « *faire de la data science sur un volume de 67 millions de gens ?* » (sic)[746].

Enfin, concernant le COMCYBER, ce dernier recrute mais a du mal à trouver des profils confirmés selon Clément Domingo. Correspondant zonal de réserve de cyberdéfense en région Occitanie pour le commandement, Yohann Bauzil indique que le recrutement de hackers éthiques se fait « *en-dessous des radars* », mais pense que le COMCYBER travaille de manière formelle avec les hackers. Yohann Bauzil a rapproché Florent Curtet du COMCYBER[747], et fait de même avec Alexandre Oda en 2019. Toutefois, en juin 2021, ce dernier s'est vu finalement annuler sa candidature car il ne pouvait justifier de performances évaluables ni de références concrètes. Certes, il n'avait pu fournir de résultats officiels issus de CTF les ayant perdus (ces niveaux de compétences commencent à être pris en compte par les autorités), mais on lui a aussi fait valoir qu'il n'avait pas de diplôme[748]. Ce qui dénote une nouvelle fois une certaine inertie administrative.

[744] Entretien avec l'auteur, 17/04/2023. D'autre avis sont plus sévères : « *Malgré ses efforts, Guillaume Poupard, l'ancien DG de l'ANSSI, est le parfait exemple que l'État reste l'État dit-il, et que ça ne changera pas*. » avance Karim Lamouri (entretien du 07/07/2023), ou encore « *Il est de bonne constitution, mais il applique des dogmes*. » selon Florent Curtet (entretien du 30/09/2021).

[745] Terme jargonneux du renseignement pour désigner le recrutement direct et informel (la DGSE organise un concours de recrutement via la fonction publique depuis 2008) d'une source par rencontre physique.

[746] Entretien avec l'autrice, 01/03/2023.

[747] Entretien avec l'auteur, 06/09/2021.

[748] Entretien avec l'auteur, 09/07/2020 et 16/06/2021. Issu de l'Armée (13e RDP) et ancien praticien du renseignement militaire, ce dernier est toutefois autodidacte en sécurité informatique. Nos demandes d'entretien avec le COMCYBER ont été infructueuses, même en passant par Yohann Bauzil que nous connaissons personnellement. Le COMCYBER s'est pourtant davantage ouvert, à la demande pressante de Guillaume Poupard (ANSSI), selon Fabrice Epelboin (entretien du 08/04/2022).

***Boussole de disposition mentale* :**

1- Posture et intentionnalité

2- Culture et intelligence

3- Patriotisme et souveraineté

4- Organisation et cohésion

***Boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité

6- Méthodes et outils

7- Intégration et synergie

8- Plasticité et agilité

Pour pousser notre analyse, nous reprenons l'analogie de la boussole et essayons d'appréhender le cap général suivi par les protagonistes de cette étude de cas.

1- Sans vision et stratégie claire de l'exécutif, les services spécialisés et de sécurité sont-ils en mesure d'influer sur la politique générale ? En dépit de l'utilisation plus naturelle du fruit de leur travail et de leurs préconisations souvent en phase avec les caps appelés par les experts en intelligence économique et la volonté de certains acteurs politiques, leur est-il possible de maintenir leur propre stratégie ? Considérons de surcroit les rivalités interservices qui doivent par ailleurs aussi s'expliquer à l'aune des difficultés à recruter des hackers.

2- La culture de la ruse et celle du renseignement est sans conteste au cœur du métier des services de sécurité. Mais une intelligence collective forte d'un esprit de *mètis* est-elle possible compte tenu des limitations juridiques et de la culture en « tuyaux d'orgue » caractéristique de ces derniers ? Les hackers, à l'inverse, ont le culte de la *mètis* et le credo du détournement et du court-circuitage.

3- Nous l'avons vu, les témoignages des hackers mettent souvent en avant un esprit patriote et le vœu d'une plus grande souveraineté, en l'occurrence en premier lieu numérique. Dans ce sens, l'État français peut-il rendre justice à cet impératif et par extension au travail de ses services de sécurité œuvrant au bénéfice du bien commun ? Par ailleurs, de leur côté, ces services créent-ils les conditions d'une confiance et témoignent-ils d'une forme de solidarité avec Florent Curtet ? Citons une nouvelle fois ce dernier et constatons ces propos édifiants : « *C'est le plus important : tu ne travailles pas à la DGSI. Et tu n'en parles à personne.* [...] *On te donnera des éléments de langage pour que tu restes évasif. Et si on nous demande qui tu es, des journalistes, des flics ou des magistrats, on ne te connait pas.* [...] *Ah, et dernière chose : on est susceptibles de couper le contact à tout moment.*[749] »

[749] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 186.

4- Quelle intégration des politiques publiques de cybersécurité, des services de sécurité et des acteurs privés spécialisés (experts SSI et hackers) qui, indépendamment de la volonté de l'État, en sont toujours plus parties prenantes ? Citons Guillaume Poupard : « *Ça prend du temps. Et, oui, il y a un côté "utilitariste". En bon technocrate, ça ne me choque pas. On veut le plus utile et efficace. Mais c'est dommage car c'est du court-terme. On a toujours peur d'être manipulé quand on ne vient pas du sérail. D'où toujours une méfiance.* »

5- Tandis que Florent Curtet, par sa position, son statut et son expertise s'inscrit pleinement dans une logique d'adaptabilité (au milieu et aux codes de la cybercriminalité et du *darkweb* notamment) et de transversalité (« entre deux mondes »), les autorités étatiques montrent une inertie administrative et un manque de maîtrise des milieux cybercriminels (créer des outils pour crawler le *darkweb* est un pas, en maitriser les codes est une autre affaire).

6- Des communautés de pratiques via notamment des outils informatiques (*pentesting*, systèmes d'exploitation, armes numériques…) existent mais les méthodes ne sont pas toujours les mêmes (infiltration analogue, ingénierie sociale) et surtout elles ne rencontrent pas les mêmes limites légales. Le fait que Florent Curtet comme d'autres (Alexandre Oda…) puissent être exploités aux fins de dépasser le cadre légal imposé aux acteurs publics est révélateur.

7- Jauger l'intégration du travail des hackers au sein des services de sécurité n'est pas chose facile. Néanmoins, il ne fait que peu de doute que les liens ténus établis (et souvent non maintenus) puissent engendrer une quelconque synergie à même de favoriser la production de connaissances actionnables. Rappelons par ailleurs, s'agissant des liens avec les organisations privées que le degré de confiance témoignée aux hackers est rarement élevé. Nous avons cité Florent Curtet se plaignant d'une forme d'hypocrisie de la part des prestataires de services de conseil concernant les résultats de leurs audits auprès de clients. Élément confirmé par Alexandre Oda citant un ami hacker qui a placé en porte-à-faux tout l'écosystème d'une entreprise toulousaine. Chargé comme *pentester* contractuel de passer après un sous-traitant en SSI de ce grand compte, il détecte de nombreuses failles non identifiées en premier lieu. Il s'est alors vu malmené, générant la zizanie dans l'environnement du groupe, lequel s'est retourné contre son sous-traitant[750].

8- Les hackers se caractérisant par leur capacité à adapter leur comportement et à influencer celui de leurs interlocuteurs (ingénierie sociale), leur agilité individuelle

[750] Entretien avec l'auteur, 09/07/2020 et 16/06/2021.

ou collective (projets communs bénévoles, appels spontanés à soutenir une cause ou remédier à une crise cyber en faveur d'ONG ou de services publics) est particulièrement utile, là où la lourdeur administrative des autorités (souvent mentionnée dans les entretiens) peut constituer un fardeau. Rappelons que Florent Curtet a fondé en un jour HWB à partir d'un évènement humanitaire (cyberattaque contre la Croix-Rouge)[751].

## Caractéristiques-clés – synthèse et hypothèses

Quels enseignements tirer de ce cas à partir des caractéristiques-clés, et ce dernier répond-il à nos hypothèses de recherche ?

• L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)

• L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)

• L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

### Synthèse :

Dans le cas qui nous occupe ici, nous avons tenté de sonder la nature et le degré des liens qui ont rapproché Florent Curtet et plusieurs services de sécurité : police et DGSI en premier lieu, ANSSI secondairement. Les impressions – certes subjectives – de celui-ci ont été enrichies des entretiens réalisés et nous avons ainsi convoqué les points de vue de professionnels et de spécialistes experts dans la thématique abordée. Les enseignements significatifs de cette analyse sont :

- Les services de sécurité sont eux-mêmes en rapport de concurrence, d'une manière générale d'abord concernant leur niveau d'expertise (rivalités picrocholines) ou leurs attributions de juridiction (Nice, Lyon, Paris, Marseille en 2007…) ; de manière particulière concernant le recrutement de hackers (DGSE, DGSI, COMCYBER)

[751] Florent Curtet, *Hacke-moi…*, *op. cit.*, p. 182. Selon Karim Lamouri, HWB a proposé son concours gracieux au nouveau directeur de l'ANSSI qui est resté lettre morte. « *C'est un pur produit de l'administration*, dit-il, *qui a fait presque toute sa carrière à l'ANSSI*. » (Entretien avec l'auteur, 07/07/2023).

- L'intérêt porté aux profils comme Florent Curtet est caractérisé par l'utilitarisme ponctuel qui témoigne d'un dilemme important quant à la gestion de ces derniers et au statut (officiel, informel, catégoriel) d'informateurs dont ils sont affublés.

- Les liens établis entre les services de sécurité et Florent Curtet (dont la nature est généralisable par la conjonction des différents témoignages d'entretiens) se révèlent pauvres, unilatéraux, empreints de méfiance et non susceptibles de pourvoir du sens à l'action du jeune hacker, ni de créer les conditions *sine qua non* à l'instauration d'un climat favorable à l'échange mutuel, à l'apprentissage et *in fine* à la production de connaissances intelligentes. Plusieurs témoignages dans nos entretiens concordent quant au désir exprimé par les hackers de rester indépendants. Cela affecte-t-il *in fine* les relations qu'ils peuvent établir avec les autorités ? Cette réflexion pose la question du désintéressement de Florent Curtet quant à sa volonté d'aider ces dernières et par extension son pays. Entrepreneur, il va de soi qu'il doive se constituer une clientèle. Toutefois, son témoignage ainsi que celui de plusieurs autres hackers ou de Pierre Penalba semblent plaider en faveur d'une démarche sincère, sans parler de ses prises de position en particulier autour des hôpitaux français, ou ses multiples initiatives bénévoles auprès de plusieurs ONG.

**Interrogations sur le cas et limites de la grille théorique :**

L'État est-il en synergie avec ses services de sécurité ? La conscience en termes de sécurité numérique se révèle limitée, on l'a vu dans la séquence qui met en cause la vigilance des plus hautes instances du pouvoir politique. Et ce en dépit des préconisations de l'ANSSI, gardienne de la cyberdéfense des ministères civils. De même lorsqu'un hacker prend l'initiative de contacter des membres du gouvernement de manière directe, inédite et inconfortable. Florent Curtet cite à cet égard des personnalités lui demandant s'il n'a pas trouvé de données compromettantes à leur sujet[752]. Ces mêmes services de sécurité sont-ils en cohérence avec un informateur du type de Florent Curtet, hacker expérimenté, patriote, bénévole et même force de propositions lors de leur collaboration ? L'ensemble des informations dont nous disposons sur ce cas nous permet-il d'inférer qu'il dénote une carence en termes de cohésion et cohérence, une absence de vision stratégique ? Il est bien entendu difficile de répondre à cette question.

Nous avons vu, par ailleurs, que si l'emploi de hackers par les services de sécurité pouvait servir des objectifs de renseignement sur la menace cyber, l'intelligence collective nécessaire pour associer les activités de cette veille avec les mesures de cybersécurité n'était pas flagrante. Encore une fois néanmoins, nous manquons de données complémentaires. L'information est-

[752] Florent Curtet, *Hacke-moi…*, *op. cit.*

elle appréhendée dans une logique cybernétique (souci d'accumulation) ou dans une perspective d'apprentissage collectif ? Si les forces de sécurité peuvent bénéficier du travail de spécialistes comme Florent Curtet, dépassant le savoir-faire de certains services (c'est acquis *a priori* et selon ce dernier pour l'ANSSI, qui estime ne pas disposer d'une telle expertise concernant du moins la cybercriminalité et ses réseaux).

Enfin, et c'est probablement ici que la grille de lecture peut s'appliquer le plus efficacement au cas, la mise en réseau d'un éventuel dispositif intelligent ne paraît pas constituer un objectif en soi ni même une intention. Les nombreux témoignages y compris d'actuels ou anciens personnels du sérail en attestent sans équivoque. On peut observer assez aisément les liens ténus et unilatéraux qui caractérisent la situation de communication très limitée entre les services comme la DGSI ou l'ANSSI et Florent Curtet. À cet égard, notre analyse pourrait être élargie en prenant le modèle systémique d'Alex Mucchielli sur les sept contextes constitutifs et constituants des situations de communication.

Des limites à l'application de notre grille de lecture sont toutefois apparues. Ainsi, il est parfois difficile de faire cadrer de manière concrète certaines caractéristiques à notre cas. Il apparaît en outre que nous ne pouvions disposer de toutes les données possibles (statut de confidentialité voire de secret, demandes d'entretiens déclinées) ou que celles-ci n'existent tout simplement pas (ex : sources secondaires, couverture médiatique inexistante). Néanmoins, en considérant les différents témoignages issus de nos entretiens (dont ceux de Florent Curtet et Pierre Penalba), notre observation empirique et notre expérience du milieu de la cybersécurité, ceci couplé aux principes de l'IE et aux préceptes de l'école de pensée sur la guerre économique, nous pouvons avancer que le cas présenté traduit un manque d'*intelligence cyber* et l'idée plausible d'une absence d'État-(cyber)stratège.

### Rappel des hypothèses :

1 – ces trois mondes (hackers–État–entreprises) sont intégrés et dans une co-construction (interaction et communication décloisonnées, projets communs, logique de dispositifs intelligents, synergie…)

2 – ces trois mondes sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas (incommunication) par manque de synergie

3 – ces trois mondes s'ignorent (acommunication)

D'un point de vue factuel, le cas étudié nous permet d'avancer que ces trois mondes sont en interaction et que, de ce fait, ils ne s'ignorent pas. Néanmoins, les rapports entretenus révèlent une forme d'incommunication parce qu'il n'y a aucune synergie ou de mise en réseau

en vue d'un projet commun concret et s'inscrivant dans une stratégie de cybersécurité. Nous pouvons donc nous positionner sur une validation raisonnable de l'hypothèse n°2.

* * *

### Résumé de l'étude de cas :

Ce quatrième cas avait trait à la trajectoire personnelle **d'un hacker au profil rare comme *chapeau noir* reconverti en *sentinelle éthique*. Il nous enseigne qu'en dépit du profil hors norme – surtout en France – et de haut niveau de Florent Curtet, les services de sécurité ont certes essayé de le recruter et d'utiliser ses réseaux et ses compétences, mais sans véritablement établir une relation pérenne et constructive : incorporation formelle à un service ou une unité, projet commun dans le cadre de missions planifiées, échanges de pratiques et de connaissances…** En définitive, des liens d'intérêt judiciaire et la rivalité interservices de la police ont eu raison de cette collaboration qui s'est du reste achevée avec fracas et sans honneur malgré les bonnes volontés manifestées par Florent Curtet. Quand bien même les services de sécurité avaient bien conscience de la plus-value de ce dernier, les dysfonctionnements de nature administrative et judiciaire et précisément l'intéressement utilitaire des institutions nous amènent à opter pour l'hypothèse n°2.

**Figure 42 :** *Tableau récapitulatif de l'étude de cas n°4*

| ***Boussole de disposition mentale :*** | **Bilan ±** |
|---|---|
| 1- Posture et intentionnalité | • Assujettissement des forces de sécurité à la posture étatique<br>• Pas de stratégie d'en haut, *idem* en bas malgré le professionnalisme |
| 2- Culture et intelligence | • Culture quasi-inhérente de la ruse chez les forces de sécurité<br>• Mais conditionnement aux limites légales et à l'organisation silotée de leurs activités |
| 3- Patriotisme et souveraineté | • Patriotisme partagé entre forces de sécurité et nombre de hackers<br>• Manque de solidarité avec les hackers malgré l'intérêt bien compris chez les forces de sécurité |
| 4- Organisation et cohésion | • Faible cohésion par esprit et intérêt utilitariste des autorités<br>• Méfiance, parfois à leur corps défendant, des forces de sécurité vis-à-vis des hackers<br>• Au bilan, pas de dispositif intelligent créé par leur mise en relation, car absence de structuration réticulaire |

| ***Boussole du dispositif opérationnel :*** | **Bilan –** |
|---|---|
| 5- Adaptabilité et transversalité | • Inertie administrative des autorités étatiques<br>• En moyenne, manque de maîtrise des milieux cybercriminels chez les forces de sécurité (codes et usages) |
| 6- Méthodes et outils | • Limitations légales des forces de sécurité dans leurs activités<br>• Malgré des communautés de pratiques et outils entre elles et les hackers |
| 7- Intégration et synergie | • Liens trop ténus entre ces deux acteurs, trop ponctuels, bilatéraux (voire unilatéraux) et utilitaires pour créer une quelconque synergie<br>• Lien similaire avec les entreprises, avec un degré de confiance limité envers les hackers |
| 8- Plasticité et agilité | • Lourdeur administrative des autorités<br>• Limites juridiques acceptées avec philosophie, bon gré mal gré, de la part des forces de sécurité |

### **5)** Bilan général des études de cas

Au long de ces quatre études de cas soumises à notre grille d'analyse, nous avons pu tirer plusieurs enseignements propres à confirmer ou infirmer nos hypothèses de départ. Trois théories ont été dégagées à partir de la démarche abductive adoptée dans le cadre de notre travail, démarche sur laquelle nous reviendrons en conclusion. Cette batterie d'hypothèses se décline en vertu de la question posée par la nature des liens entre les hackers et les autorités étatiques et organisations privées. La première part de l'idée (positive) que ces acteurs communiquent dans le cadre d'une coopération poussée qui ferait penser que ces interactions (*communication*) auraient abouti à un dispositif intelligent (moyen/stratégie), donc intégré et synergique propre à assurer (objectif/politique) un niveau élevé de cybersécurité. La troisième hypothèse constitue l'idée (négative) opposée à la précédente, à savoir que ces acteurs ne communiquent pas (*acommunication*) car ils iraient jusqu'à s'ignorer voire se mépriser. La deuxième théorie, enfin, vient en position médiane nuancer ces deux réalités extrêmes en émettant l'idée (insuffisante/encourageante) que bien qu'en interaction voire coopération, ces acteurs communiquent peu/mal (*incommunication*) ou se comprennent difficilement, engendrant des interférences préjudiciables à tout projet synergique co-établi et empêchant ainsi l'émergence d'un dispositif intelligent (de fait *perturbé*). Ce point rappelé, reprenons dès lors les études de cas considérées.

En premier lieu, **le cas *Bluetouff* nous a permis de comprendre que les codes des hackers sont difficiles à appréhender pour les institutions judiciaires**. Mis à part les avocats spécialisés contraints de s'y pencher ou par appétence pour le domaine, le fonctionnement des seules technologies numériques est étranger à la plupart des magistrats. Que dire dès lors d'une éthique hacker régie par la *do-ocratie* et selon laquelle la capacité d'action et de faire est érigée en principe philosophique fondamental ? Cet état de fait engendre des situations où la communication entre acteurs aux référentiels très différents éprouvent des difficultés à se comprendre. Enfin, le cas étudié donne cependant à observer que les services de sécurité (SR, police, gendarmerie) partagent des méthodes et des outils de travail (TIC/informatique) voire une certaine accointance d'esprit avec les hackers. Nous en sommes donc venu à valider l'hypothèse médiane numéro 2.

S'agissant du **deuxième cas**, en lien avec cette fois le regard politico-législatif porté sur les hackers, l'on retiendra qu'il **vient conforter les leçons tirées de l'affaire relative au premier cas, puisque des aménagements législatifs corrigent l'étroitesse de la loi en la matière. Tout en laissant, cependant, encore un flou règlementaire dû à la difficulté pour la classe politique à comprendre réellement l'utilité de considérer les hackers comme des piliers de la cybersécurité**. Sans hackers, qui pour faire remonter les failles et les tester, hormis des spécialistes de sécurité informatique dont le métier est la recherche, les RSSI ayant évidemment déjà bien à faire pour sécuriser leur propre organisation ? La classe politique est bien consciente du risque cyber mais n'a qu'une faible culture dans le domaine. Elle est souvent, à l'image du grand public, happée par les aspects fascinants et tendanciels des technologies numériques. Malgré tout, le niveau de cette inculture cyber n'est pas homogène et certaines initiatives individuelles sont à saluer, qui proposent des projets encourageants. Eu égard à ces considérations, nous avons validé l'hypothèse n°2.

**Le troisième cas portait, quant à lui, sur les cyberattaques régulièrement subies par les centres hospitaliers français. Deux enseignements focaux ont été retenus : d'abord, que les établissements de santé manquent de ressources financières et qu'à l'image des autres institutions publiques et dans une certaine mesure privées, la part de leur budget alloué aux SI et plus encore à leur sécurité était négligeable ; ensuite, que pour des raisons compréhensibles mais dans le même temps synonymes de grande vulnérabilité, les personnels soignants manquent d'une culture de sécurité, ce qui induit une surface d'attaque élargie ouverte à la cybermenace**. Cette cybercriminalité charognarde faisant montre d'un opportunisme aigu, les hôpitaux deviennent des proies évidentes. En l'absence de hackers dans

ce contexte, mais du fait des besoins orientés vers ce genre de profils et des réactions synergiques en réponse aux crises, nous avons donc embrassé les hypothèses n°1 & 2.

**Enfin, le quatrième cas avait trait à la trajectoire personnelle d'un hacker au profil rare comme *chapeau noir* reconverti en *sentinelle éthique*. Il nous enseigne qu'en dépit du profil hors norme – surtout en France – et de haut niveau de Florent Curtet, les services de sécurité ont certes essayé de le recruter et d'utiliser ses réseaux et ses compétences, mais sans véritablement établir une relation pérenne et constructive : incorporation formelle à un service ou une unité, projet commun dans le cadre de missions planifiées, échanges de pratiques et de connaissances…** En définitive, des liens d'intérêt judiciaire et la rivalité interservices de la police ont eu raison de cette collaboration qui s'est du reste achevée avec fracas et sans honneur malgré les bonne volontés manifestées par Florent Curtet. Quand bien même les services de sécurité avaient bien conscience de la plus-value de ce dernier, les dysfonctionnements de nature administrative et judiciaire et précisément l'intéressement utilitaire des institutions nous amènent à opter pour l'hypothèse n°2.

**Figure 43 :** *Tableau récapitulatif de l'ensemble des études de cas*

| **Étude de cas n°1 : affaire Bluetouff** | |
|---|---|
| ***Boussole de disposition mentale*** | **Bilan – (Justice) ; Bilan ± (forces de sécurité/avocats)** |
| 1- Posture et intentionnalité | • Référentiels différents entre hackers et autorités judiciaires, rares magistrats spécialisés<br>• Connaissance des TIC chez les avocats spécialisés, eux très nombreux |
| 2- Culture et intelligence | • Culture du numérique et *a fortiori* de la sécurité informatique défaillante chez les magistrats<br>• Les hacktivistes sont considérés comme les meilleurs de leurs coreligionnaires (par rapport aux hackers *blancs*) mais sortent souvent du cadre légal |
| 3- Patriotisme et souveraineté | • Défaut de souveraineté et de « patriotisme numériques »<br>• Utilisation d'outils étrangers, dépendance technologique des forces de sécurité françaises |
| 4- Organisation et cohésion | • Amélioration du schéma organisationnel de sécurité depuis l'affaire<br>• Mais manque de cohésion générale et signaux divergents émis par les différentes institutions |
| ***Boussole du dispositif opérationnel*** | • **Bilan – (Justice) ; Bilan ± (forces de sécurité)** |
| 5- Adaptabilité et transversalité | • Inadaptation et décalage du monde judiciaire<br>• Pas de vision commune avec les autorités de sécurité |

| | |
|---|---|
| 6- Méthodes et outils | • Méconnaissance manifeste des TIC chez les magistrats<br>• Communauté de pratiques entre hacktivistes et forces de sécurité |
| 7- Intégration et synergie | • Absence de coordination entre autorités sécuritaires et judiciaires quant au regard porté sur un hacktiviste comme *Bluetouff*<br>• *A priori* négatif vis-à-vis des profils hacktivistes |
| 8- Plasticité et agilité | • Point de vue des magistrats figé sur le droit<br>• Difficulté voire impossibilité à sortir de ce cadre rigide |
| **Étude de cas n°2 : la classe politique** | |
| ***Boussole de disposition mentale :*** | **Bilan −/± (classe politique) ;<br>Bilan + (certaines entreprises)** |
| 1- Posture et intentionnalité | • Manque de connaissance de ses propres forces de la part de l'État<br>• Absence de vision stratégique |
| 2- Culture et intelligence | • Manque de culture cyber et de sécurité chez les élites politiques<br>• Au contraire des anciens des SR qui créent leur entreprise<br>• Entreprises françaises généralement peu acculturées elles aussi. |
| 3- Patriotisme et souveraineté | • Intérêt et inquiétudes (tardifs et épisodiques) pour la souveraineté numérique chez les politiques<br>• Pas de cadre stratégique étatique pour accompagner la posture patriotique de nombreux hackers et leur volonté d'agir<br>• Contacts entre SR et hackers mais non structurés et seulement à titre individuel |
| 4- Organisation et cohésion | • Manque de liant et d'une interface entre hackers et autorités<br>• Verrous juridiques et politiques, voire conflits d'intérêts chez les élites |
| ***Boussole du dispositif opérationnel :*** | **Bilan ± (classe politique) ;<br>Bilan ± (forces de sécurité)** |
| 5- Adaptabilité et transversalité | • Immobilisme important chez la classe politique<br>• Mis à part certains acteurs et initiatives individuelles |
| 6- Méthodes et outils | • Communautés de pratiques entre civils/militaires, hackers/forces de sécurité (convergence technique)<br>• Communauté d'intérêt en revanche relative : patriotisme commun avec les forces de sécurité, valeurs moins évidentes chez les politiques. |
| 7- Intégration et synergie | • Pas de structuration d'une interface de dialogue entre hackers et politiques<br>• Mauvaise compréhension de la plus-value des hackers chez les élites politiques<br>• Pas de synergie avec l'État, communication ponctuelle avec les hackers |
| 8- Plasticité et agilité | • Lourdeur des structures du pouvoir politique<br>Absence de stratégie au niveau de l'État pointée par de nombreux interviewés |

| **Étude de cas n°3 : les hôpitaux** | |
|---|---|
| ***Boussole de disposition mentale :*** | **Bilan ±** |
| 1- Posture et intentionnalité | • Manque de préparation face aux attaques<br>• Pas d'audits en amont pour évaluer le risque cyber au mieux, la cyber-résilience au pire |
| 2- Culture et intelligence | • Manque d'acculturation…<br>• et de sensibilisation/éducation au risque cyber |
| 3- Patriotisme et souveraineté | • Posture d'intelligence économique faible<br>• Traitement (considération ?) par l'État des établissements hospitaliers comme services publics faible<br>• Pas d'accompagnement d'initiatives pourtant bénévoles de certains hackers au chevet des hôpitaux |
| 4- Organisation et cohésion | • Cohésion d'équipe face au risque cyber ponctuelle car conditionnée aux attaques subies<br>• Satisfaction collective après la mutualisation des moyens, compétences et dynamisme, mais lors de crises cyber<br>• Sécurité physique également faible au-delà des aspects informatiques |
| ***Boussole du dispositif opérationnel :*** | **Bilan ±** |
| 5- Adaptabilité et transversalité | • Réactivité mais non proactivité de l'État face aux cyberattaques contre les hôpitaux<br>• Mutualisation des forces ponctuelle et non continuelle chez ces derniers |
| 6- Méthodes et outils | • Compétences axées sur la défense donc manque d'anticipation des RSSI des centres de santé face aux pirates<br>• Faiblesse générale des établissements en termes de sécurité informatique |
| 7- Intégration et synergie | • Manque de compréhension mutuelle de chaque métier<br>• Manque de dialogue avec et d'intérêt porté aux équipes d'informatique |
| 8- Plasticité et agilité | • Inadaptation des personnels soignants aux mesures et règles de sécurité<br>• Mais prise de conscience de ce problème pendant et après une crise/attaque |
| **Étude de cas n°4 : Florent Curtet** | |
| ***Boussole de disposition mentale :*** | **Bilan ±** |
| 1- Posture et intentionnalité | • Assujettissement des forces de sécurité à la posture étatique<br>• Pas de stratégie d'en haut, *idem* en bas malgré le professionnalisme |
| 2- Culture et intelligence | • Culture quasi-inhérente de la ruse chez les forces de sécurité<br>• Mais conditionnement aux limites légales et à l'organisation silotée de leurs activités |
| 3- Patriotisme et souveraineté | • Patriotisme partagé entre forces de sécurité et nombre de hackers<br>Manque de solidarité avec les hackers malgré l'intérêt bien compris chez les forces de sécurité |
| 4- Organisation et cohésion | • Faible cohésion par esprit et intérêt utilitariste des autorités |

| | |
|---|---|
| | • Méfiance, parfois à leur corps défendant, des forces de sécurité vis-à-vis des hackers<br>• Au bilan, pas de dispositif intelligent créé par leur mise en relation, car absence de structuration réticulaire |
| ***Boussole du dispositif opérationnel :*** | **Bilan –** |
| 5- Adaptabilité et transversalité | • Inertie administrative des autorités étatiques<br>• En moyenne, manque de maîtrise des milieux cybercriminels chez les forces de sécurité (codes et usages) |
| 6- Méthodes et outils | • Limitations légales des forces de sécurité dans leurs activités<br>• Malgré des communautés de pratiques et outils entre elles et les hackers |
| 7- Intégration et synergie | • Liens trop ténus entre ces deux acteurs, trop ponctuels, bilatéraux (voire unilatéraux) et utilitaires pour créer une quelconque synergie<br>• Lien similaire avec les entreprises, avec un degré de confiance limité envers les hackers |
| 8- Plasticité et agilité | • Lourdeur administrative des autorités<br>• Limites juridiques acceptées avec philosophie, bon gré mal gré, de la part des forces de sécurité |

* * *

Au bilan, ces études de cas se sont révélées fécondes quant à leurs enseignements malgré certaines craintes initiales sur le degré d'informations utiles qui en procèderait. Recoupées par les riches témoignages obtenus dans le cadre des entretiens menés en parallèle, nous pouvons en dégager **plusieurs points d'ordre général en lien avec notre problématique de recherche : un manque de constance et d'unité ; un paradoxe ; une forme d'incohérence.**

*Primo*, **on note un évident manque de cohésion sinon de cohérence dans le rôle qu'on peut accorder aux hackers dans la politique de sécurité numérique nationale**. Leur statut est encore flou et surtout pas assez protégé. D'une manière générale, si l'on note les avancées en termes de cyberdéfense d'un côté et dans une moindre mesure sur le plan de la cybersécurité, on constate également le cloisonnement entre les deux sphères, et une certaine propension à élaborer une stratégie par le MINARM, peu de passerelles étant jetées entre celle-ci et la stratégie de sécurité du numérique de 2015. Là où du reste, la première a été étoffée au fil des ans, la seconde n'a pas fait l'objet d'une actualisation. Seule une directive européenne (NIS2) doit venir prochainement élargir son périmètre d'application de protection et améliorer la coordination avec les autres membres de l'Union européenne. Par ailleurs, il faut noter que les acteurs publics de l'écosystème de cybersécurité connaissent des interférences dans leur coordination. En mars 2023, un rapport de la Cour des comptes a notamment déploré la relégation subie par le Groupement d'intérêt public (GIP) *Action contre*

*la cybermalveillance* (ACYMA[753]), lequel apporte son assistance aux victimes de cyberattaques. L'ACYMA manquerait cruellement de budget et ses attributions viendraient buter contre les différentes architectures de l'écosystème. Le Sénat est venu appuyer ce constat dans un rapport d'information intitulé *Pour une Coordination de la cyberdéfense plus offensive*, en requérant une clarification des rôles entre ANSSI, CSIRT régionaux ou sectoriels et GIP ACYMA[754].

*Secundo*, **il y a un paradoxe dans la connivence intellectuelle, au moins par le biais d'une passion commune, entre les hackers et les plus spécialistes du domaine parmi les forces de sécurité**. L'exemple de l'amitié qui lie Florent Curtet à son « tortionnaire » originel, Pierre Penalba, est significatif, de même quand le premier évoque les profils parfois très similaires que l'on trouve pourtant chacun d'un côté ou l'autre de la barrière. Tandis que la classe politique, servie avec un sens du devoir et tant de déférence par les forces de sécurité, mécomprend les ressorts fondamentaux qui animent les hackers dont beaucoup font pareillement preuve d'engagement patriote.

*Tertio*, **et comme corollaire avec le point précédent, est-ce l'un des facteurs qui poussent les autorités de sécurité à traiter de manière intéressée les hackers, dans une logique de résultats notamment court-termistes ?** Le cas spécifique des hacktivistes (comme celui de *Bluetouff*) peut certes interroger, et demanderait probablement de les étudier au cas par cas pour s'assurer de leurs intentions. Ceci étant, s'il a été inquiété par deux fois au moins par la Justice, Olivier Laurelli a aussi été sollicité dans le cadre très formel et officiel d'enquêtes parlementaires. D'abord pour apporter un éclairage quant à l'ancienne loi HADOPI, mais surtout en 2021 dans le cadre de la mission d'information sur la souveraineté numérique française et européenne. Il y a été notamment auditionné pour participer à un débat contradictoire – particulièrement bienvenu – avec le président de Palantir France, l'ex-PDG d'Airbus Helicopter, Fabrice Brégier[755].

* * *

Après avoir établi que le contexte de cyberguerre s'inscrivait dans la toile de fond de la guerre systémique, et qu'il fallait donc adopter une posture adossée à celle de l'intelligence économique, nous allons expliquer notre concept d'intelligence cyber et formuler des recommandations pour le mettre en pratique.

[753] https://www.cybermalveillance.gouv.fr/

[754] https://www.senat.fr/rap/r22-638/r22-6385.html#toc37. Voici ses constats : « *La mise en place des CSIRT régionaux s'est faite sur la base d'un volontariat des régions et selon un modèle assumé comme "expérimental" par l'ANSSI ; La pérennité du financement des CSIRT n'est pas assurée au-delà de l'amorçage du Plan de relance ; Les régions alertent sur le risque de devoir seule*[s] *assumer la charge du dispositif alors qu'il s'agit d'une mission régalienne.* »

[755] https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

# Chapitre 6 | Vers une intelligence cyber

« *Face à la situation, la stratégie saute aux yeux.* »

Poème *Zaofa*, de Zong Ze (dynastie Song)

**Il y a comme un paradoxe à propos de l'intelligence économique, du moins dans son approche polémologique : elle est en effet d'abord une stratégie-outil fondée sur un constat pragmatique du réel ; mais elle porte aussi en elle une vision idéale car elle se veut prescriptrice pour améliorer ce réel. En vérité, elle s'inscrit simplement dans ce qu'appelait le géographe Paul Vidal de la Blache le « possibilisme »**. À savoir, la marge de manœuvre que peut se donner l'Homme pour faire face aux fatalités de la géographie. Précisément, c'est l'Histoire qui autorise ce dernier à écrire une syntaxe des évènements. Or, cette possibilité de faire, c'est avant tout la volonté d'agir. Face au déterminisme apparent des jeux de l'économie et de la compétition globale, notre pays, cet *homme souffrant de l'Europe*, peut se rétablir. Pour paraphraser et adapter Spinoza, le cyberespace constitue le champ augmenté de la puissance et de l'influence[756]. Or, le diagnostic déterministe du philosophe néerlandais signifiait en réalité la liberté donnée à l'Homme de s'extraire de ses illusions.

Tel est le premier pas à effectuer pour agir et ne plus subir. À cet égard et en premier lieu, restaurer la souveraineté de la France passera par le numérique. Or, si tout ou presque est à faire s'agissant du code, le monde des hackers et notamment son continent du logiciel libre peut être un point d'appui et de départ voire un tremplin. La gendarmerie n'a-t-elle pas montré la voie, elle qui se trouve entravée par les problèmes d'interopérabilité avec les logiciels privateurs dont la France a, en définitive, fait la promotion au profit de marques étrangères et tout particulièrement américaines ?[757] Facteur d'un pouvoir sinon égalisateur du moins *challengeur*[758] (contestateur), le cyber permet aux puissances en devenir ou en recul comme notre pays de rétablir l'équilibre des masses critiques. Notre « puissance d'équilibre » doit précisément permettre des points de bascule. Cela passe par l'innovation du privé et son accompagnement permanent et systématique par la puissance publique et souveraine. Par l'éducation et la formation, où beaucoup est à faire pour forger un esprit critique face aux TIC et aux réseaux socionumériques, sensibiliser et infuser une culture du renseignement et de la

[756] La citation originale de Baruch Spinoza est : « *L'espace est le champ de la puissance des hommes ; le temps est celui de leur impuissance*. » (*Éthique*, 1677).

[757] Les clouds et solutions de partage collaboratif américains (Amazon Web Service (AWS), OneDrive de Microsoft, GoogleDrive d'Alphabet) utilisés par les particuliers, entreprises et l'administration française. La suite logicielle Office 365 de Microsoft équipant un très grand nombre d'établissements supérieurs privés, etc.

[758] Olivier Martin, « Le mythe du "pouvoir égalisateur du cyber" », *Revue Défense Nationale*, 2019/8 (N° 823), pp. 71-75.

sécurité. Enfin, cela nécessite le décloisonnement des forces vives et l'intégration de tous les acteurs, et parmi eux les hackers patriotes.

## A. *L'intelligence au service d'une vision globale du cyber*

> « *Le cyber constitue une révolution et agit comme un levier amplificateur d'effets. Sa prise en compte n'est pas une question mais une nécessité, au risque de perdre une liberté d'action et une autonomie stratégique.* »
>
> CNE Olivier Martin

De la même manière que sur fond de guerre économique l'IE procure l'esprit et un instrument stratégiques, pour mener celle du cyber il y a lieu de convoquer une posture et un outil à travers une *intelligence cyber*, par-delà une cyberstratégie strictement militaire. Il s'agit dès lors d'appliquer les ressources et méthodes de l'IE au cyber tout en tenant compte de ses spécificités. Si les tenants de l'IE en France invoquent un positionnement plus offensif de l'État[759], l'intelligence cyber requiert pareillement une dynamique dans laquelle le pays dépasserait son attitude réactive traditionnelle. Ainsi, il est désormais temps d'augmenter notre approche de sécurité numérique et de cyberdéfense pour passer à une véritable *cybersécurité offensive*, où acteurs publics et privés mutualisent leurs objectifs et moyens dans un horizon stratégique commun. Si le temps presse, il n'est pas trop tard. Le pays peut compter sur des moyens propres et certes opérer les virages des révolutions technologiques à venir comme le quantique et l'IA. Mais il doit aussi combler les manquements de base dans les logiciels. Cela passe par un sursaut de souveraineté numérique. Les appels d'acteurs privés nationaux vont dans ce sens.

### 1) Les apports de l'intelligence économique au cyber

La grille de lecture fondée sur la modélisation des caractéristiques de l'IE a permis de poser un cadre d'analyse à l'aune duquel ont été appréhendés les rapports entretenus entre hackers et organisations publiques et privées. Ce parti pris initial mais autocritique s'est vu conforter par la démarche abductive suivie et les mouvements de va-et-vient opérés entre nos hypothèses et les données empiriques et d'observation immersive – ou d'immersion observatrice – sur lesquelles cette grille a été plaquée et testée. Science de l'action construite

[759] Voir notamment : Christian Harbulot, Nicolas Moinet, Arnaud de Morgny (dir.), *Guerre économique : comment gagner ?*, Nouveau Monde Éditions, 2023, 180 p. ; https://www.epge.fr/enfin-un-rapport-sur-lintelligence-economique-qui-aborde-la-question-de-loffensive/ ;https://www.archimag.com/veille-documentation/2023/02/28/ies-2022-plaidoyer-pour-intelligence-economique-offensive; https://www.senat.fr/travaux-parlementaires/commissions/commission-des-affaires-economiques/intelligence-economique.html.

et constructive, état d'esprit et culture résumée à l'image d'un triptyque *vigie-bouclier-épée* ou encore *chouette-mangouste-renard* pour tisser la métaphore animale – comme on voudra –, l'IE est bien placée pour évaluer le niveau de maîtrise de l'information et le degré d'interaction communicante entre différents acteurs. En effet, de ses différents concepts théoriques et de l'expérience opérationnelle issue de son application pratique dans les entreprises ou les collectivités territoriales, elle permet de nourrir la réflexion pour juger de l'efficacité ou non d'un acteur, de son absence ou non de vision stratégique. Or, le cyber augmente simplement mais en les complexifiant tous les enjeux discutés et embrassés par l'intelligence économique. Ainsi, l'IE s'avère une grille de lecture tout à fait pertinente pour sonder le degré de cohésion et cohérence, de synergie et mise en réseau autorisant une intelligence du cyber. Elle a donc permis de tirer des enseignements quant aux carences du dispositif et des politiques de cybersécurité nationale.

Nous nous sommes appliqué à modéliser l'IE selon six principales caractéristiques reposant sur une approche d'abord théorique et philosophique, puis à l'aune de la réalité opérationnelle de la discipline. Pour compléter cette modélisation, a été conçue une approche en quelque sorte azimutale où l'analogie de la boussole est convoquée pour mieux saisir les principes théoriques et pratiques de l'IE. Enfin, nous avons tenté de synthétiser l'ensemble de ces éléments référentiels pour en tirer trois caractéristiques-clés. Par souci de précision, voici rappelé ci-dessous l'appareillage théorique :

***Disposition mentale***

1ère caractéristique : un domaine de réflexion interdisciplinaire qui s'appuie sur le paradigme de la complexité pour appréhender le réel et le « village global »

2e caractéristique : science en action et culture de l'intelligence rusée

3e caractéristique : une posture de combat fondée sur le triptyque patriotisme–unité–souveraineté

***Dispositif opérationnel***

4e caractéristique : une posture managériale transversale qui place l'information au centre du jeu stratégique

5e caractéristique : méthode opérationnelle globale de maitrise de l'information reposant sur trois champs d'activité : veille, sécurité et influence

6e caractéristique : un processus réticulaire basé sur des dispositifs intelligents visant l'agilité stratégique

***Boussole de disposition mentale* :**

1- Posture et intentionnalité

2- Culture et intelligence

3- Patriotisme et souveraineté

4- Organisation et cohésion

***Boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité

6- Méthodes et outils

7- Intégration et synergie

8- Plasticité et agilité

***Caractéristiques-clés***

• L'IE se distingue d'abord par son engagement philosophique et stratégique (elle est intentionnalité-volonté, praxis, cohésion-cohérence)

• L'IE se distingue ensuite par son usage transversal d'outils synthétisés en un triptyque dont le pivot est l'information (elle est préhension, analyse, opérationnalisation)

• L'IE se distingue enfin et surtout par sa méthode réticulaire de production de connaissances actionnables (elle est dispositif, communication, synergie).

Bien qu'elle ne soit pas une philosophie et un outil adoptés et déployés d'une manière uniforme, l'IE apparait toutefois comme un excellent agent révélateur d'un instantané situationnel. Elle permet en effet de jauger le degré de posture vigilante, défensive et offensive d'un acteur politique, économique ou même individuel. Rapporté à l'échelle nationale, un dispositif supposé stratégique trouve ainsi une résonnance au prisme de l'IE comme grille d'analyse. L'on peut ainsi évaluer cet acteur dans sa propension à l'agilité, sa capacité à faire lien/à relier, sa disposition à évoluer dans un cadre d'échange structuré mais flexible, son rapport à l'intérêt général, sa volonté enfin de fixer un cap stratégique et tracer une voie pour atteindre ses objectifs. L'on remarquera du reste, dans un sens critique, que les dispositions mentales et opérationnelles sont comparables aux traditionnelles dialectiques théorie/empirie, nature/culture, esprit/corps ou encore interne/externe, voire – c'est le sens de L'IE – politique/économique : elles sont vraisemblablement artificielles. Effectivement, elles exigent au pire ou découlent au mieux d'une conjonction entre une conceptualisation/intention/compréhension et une opérationnalisation/action/préhension. En somme, pour citer le psychologue Kurt Lewin, « *rien n'est plus pratique qu'une bonne théorie* ».

Ainsi, en associant ces trois ensembles dans la modélisation de la grille de lecture, nous obtenons un appareillage propre à sonder de manière compréhensive les cas sélectionnés ainsi

que nos données empiriques : émergement de trois caractéristiques centrales présentes à l'esprit que le *corps* met en œuvre à travers trois caractéristiques de l'action ; dézoom pour une prise de hauteur afin de juger du cap stratégique (boussole) ; enfin, synthèse affinée pour obtenir trois caractéristiques-clés.

Pour conclure cette section, nous proposons une analyse de matrice SWOT – outil issu des sciences de gestion – pour synthétiser les enseignements tirés de la partie 2 et qui servira de base à nos préconisations à venir.

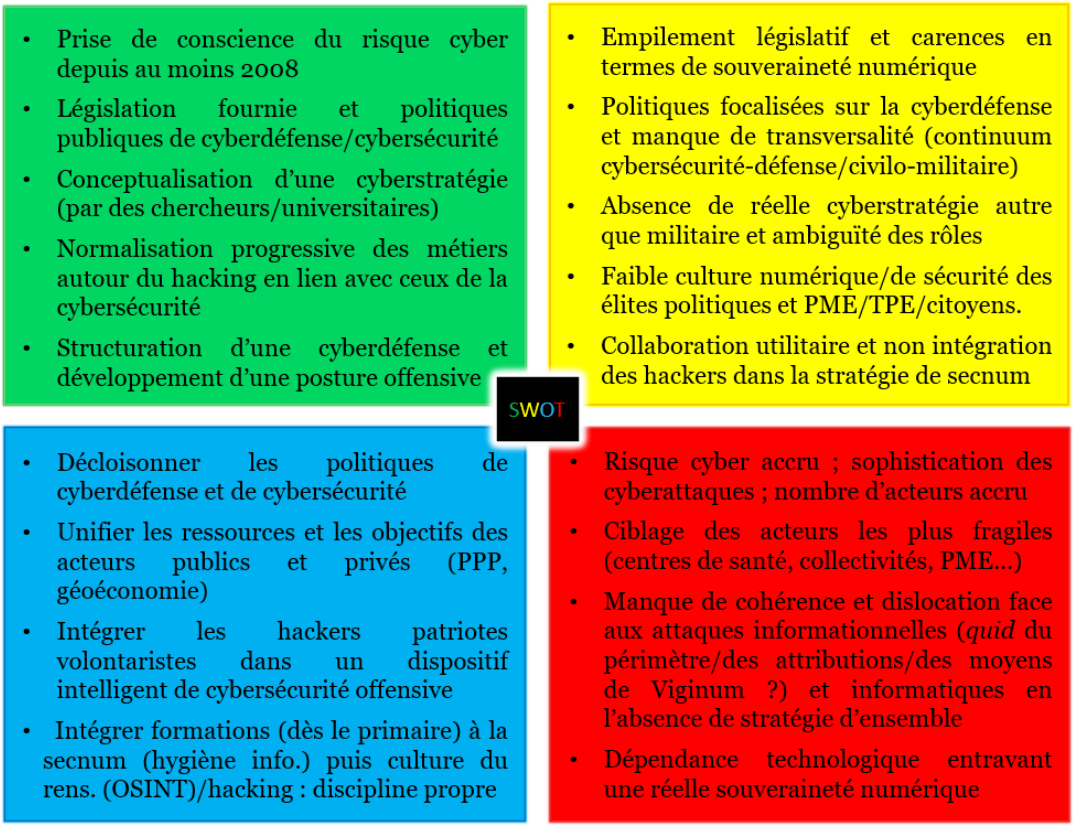



**Figure 44 :** *Modèle SWOT présentant l'analyse synthétique de la politique de sécurité numérique en France*

Source : Yannick Pech, 2023.

Après avoir résumé la démarche d'élaboration de notre grille théorique et justifié sa pertinence, il convient désormais d'expliciter le concept d'intelligence cyber, lequel se fonde sur une approche pragmatique de la cyberconflictualité et une posture offensive.

## **2)** L'intelligence cyber, entre stratégie défensive et offensive

« *Les évènements qui doivent se produire finissant toujours par se produire, ce que nous devons et pouvons faire, c'est nous demander comment obtenir la victoire*. »

Qiao Liang & Wang Xiangsui

Si la meilleure cyberdéfense n'est pas à coup sûr la cyberattaque, la prime revient généralement à celui qui prend les devants. Dans tous les cas, à l'image du jeu de Go, la victoire est conditionnée à la capacité de conserver l'initiative (*sente* en japonais). Deux types d'enchainement de coups déterminent le jeu : soit la distribution spatiale/scalaire des pions (pierres) en vue de déployer son influence à partir d'une zone du *goban*, soit l'attaque en quelque sorte « *latérale-frontale* »[760] évoquée par les généraux Wang Xiangsui et Qiao Liang et consistant à s'approcher d'une pierre adverse ou d'envahir sa zone d'influence. En définitive, la prise d'initiative est toujours récompensée car on impose son rythme à l'adversaire qui, dépassé (*gote*), perd son énergie à seulement contrer les attaques et limiter les dégâts. Or, généralement, le joueur en possession du *sente* en fin de partie la gagne. Qu'en est-il dans le réel et le cyberespace ? Eh bien, la boucle OODA ou la théorie des *échiquiers invisibles* ne disent pas autre chose[761].

Si le cyber est une modalité complémentaire de la conflictualité – militaire du point de vue de la politique française –, il « *signe aussi et surtout l'avènement d'une forme nouvelle de conflictualité*.[762] ». La cyberguerre est, à travers les attaques informatiques et informationnelles, l'enjeu du contrôle et de l'influence. Et le cyberespace est, à n'en pas douter, une sorte de *no man's land* situé entre les relations diplomatiques et la guerre ouverte, un lieu permanent de la conflictualité de tout le monde contre tout le monde. Henri Kissinger n'a-t-il pas dit que l'espace numérique était l'illustration parfaite de « l'état de nature », requérant une régulation globale qui pourtant ne vient pas ? Pour l'heure, c'est donc la jungle 2.0. Deux options s'offrent à nous, proies ou chasseurs : on la subit ou l'on s'y adapte. D'abord, dépasser la conception strictement militaire de la cyberdéfense. Ensuite, penser plutôt cybersécurité, intégrale et *offensive*.

### **a)** ***« La militarisation de tout »***

Rejoignant la maxime de Trotski selon laquelle si l'on ne s'intéresse pas à la guerre, cette dernière s'intéresse quand même à nous, puis l'approche de la *guerre hors limites*[763],

[760] Qiao Liang & Wang Xiangsui, *op. cit.*, *passim.*
[761] Christophe Deschamps & Nicolas Moinet*, La boîte à outils de l'intelligence économique*, Dunod, 2017, 192 p.
[762] Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber…*, *op. cit.*, p. 5.
[763] Qiao Liang & Wang Xiangsui, *op. cit.*

l'historien Mark Galeotti consacre lucidement la réalité d'une guerre systémique[764]. Dans cette perspective, la guerre s'est justement « démilitarisée ». Elle est vouée à se diluer tout autant voire plus dans la sphère civile des sociétés humaines. Dès lors, une cyberdéfense devient caduque. La vision chinoise est tout à fait claire et cohérente à ce propos :

> « *Cette vision pan-domaines est une des conditions de la survie et du développement des États souverains modernes ainsi que de leur influence dans le monde. En comparaison, la vision de la défense nationale comme principal objectif de la sécurité apparaît assez dépassée, à la rigueur très incomplète. À cette vision pan-domaines, on doit faire correspondre une nouvelle notion de sécurité omnidirectionnelle incluant les intérêts de l'État. Ce sur quoi elle met l'accent ne se limite absolument pas aux questions de sécurité et de défense : elle comprend aussi dans sa zone d'intervention la sécurité politique, la sécurité économique, la sécurité culturelle et la sécurité de l'information. Il s'agit d'une vision sécuritaire étendue qui élève la notion traditionnelle de domaine territorial à la notion de domaine de l'intérêt de l'État.* […] *comment faire face à des pirates informatiques qui vont et viennent sur Internet ? La conclusion coule de source : il ne suffit pas de posséder une épée pour garantir la sécurité nationale dans le champ d'une vision sécuritaire étendue. Comme le dit le proverbe, "un pilier ne soutient pas la maison". L'unique pilier de l'armée est loin de pouvoir soutenir la voûte sécuritaire de l'édifice national moderne. La solution qui l'empêchera de s'effondrer réside pour une bonne part dans la capacité de constituer une force composite regroupant tous les domaines qui touchent à l'intérêt national.* […] *Ce que tous les militaires et politiciens qui nourrissent la folle ambition de remporter des victoires devront faire, c'est élargir leur champ de vision, évaluer le moment et la situation, saisir le bâton de la grande stratégie et écarter les miasmes de la vision guerrière traditionnelle, bref : aller de l'autre côté de la montagne pour accueillir le soleil levant.*[765] »

Y compris sur le seul plan militaire, l'approche française de la sécurité est-elle conçue d'après une vision si élargie ? Cette vision chinoise, même adaptée, est-elle inconcevable pour une démocratie comme la nôtre ? Les officiers chinois Wang Xiangsui et Qiao Liang ne font pourtant rien d'autre que s'appuyer sur la stratégie américaine, avec en 1999 une admiration à peine dissimulée. Le titre de leur ouvrage *La guerre hors limites* élude par la forme un aspect pourtant fondamental, qu'ils développent par le menu dans le texte : la guerre doit être « combinée », c'est-à-dire faire flèche de tout bois, articuler tous les moyens défensifs et offensifs. En somme, élaborer une stratégie globale de long-terme. Rapporté au cyber, une ligne Maginot numérique est-elle donc suffisante pour lutter à armes égales contre nos adversaires ? Nous devons nous appuyer sur la vision du général Burkhard mais la transcender pour assurer une cybersécurité intégrale. Cet appel en 2020 de plus de cinquante personnes

[764] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 2022, 248 p.

[765] Qiao Liang & Wang Xiangsui, *ibid.*, pp. 170-173. Ancien secrétaire de la Défense et professeur à Stanford, William J. Perry dira de l'informatique qu'elle a répondu à la question que les soldats se posaient depuis des centaines d'années, à savoir : qu'est-ce qu'il y a de l'autre côté de la montagne ? Cité par Qiao Liang et Wang Xiangsui, *idem*, p. 173, note 1.

issues de la communauté des hackers ou experts en cybersécurité, dirigeants d'entreprises et députés constitue une première revendication à portée nationale[766]. Inquiets de la dépendance numérique à des pays tiers que subit la France, les signataires de cette pétition réclament une véritable stratégie nationale numérique fondée sur la création d'un ministère dédié avec comme priorité d'assurer la souveraineté technologique et de placer la cybersécurité au cœur de cette politique. Ces cinquante-quatre personnalités plébiscitent un « *projet transverse aux actions publiques et aux activités privées* » axé sur un triptyque « *sécurité-souveraineté-influence* ». Une façon de placer la France en ordre de bataille et d'envisager enfin une posture offensive.

### b) *Adopter une cybersécurité offensive*

La cybersécurité dite offensive est l'approche du domaine consistant à se glisser dans la peau de l'attaquant pour mieux s'en défendre. Voilà pourquoi elle est presque invariablement associée aux hacking éthique. Plus qu'une sécurité « active » et une vigilance, il s'agit de se montrer proactif, à l'image de la « *stratégie américaine de persévérance et de confrontation continue (*Persistent Engagement*)* [qui] *doit permettre de contrer les menaces à leur source (*Defend Forward*), d'augmenter la sécurité* [du pays] *et de conforter* [sa] *position*.[767] » Si cette doctrine présente des défauts et des limites, en adapter l'esprit et aménager la lettre en concordance avec notre vision nationale pourrait au moins servir d'aiguillon.

Cette approche offensive fait défaut en France, et le travail isolé de la DGSE en sus des initiatives du COMCYBER ne doivent pas nous faire oublier qu'une telle posture doit être globale, civile et militaire, publique et privée et en outre pas seulement technique. Pour mener ces guerres de l'information au sens large, il est nécessaire de penser « hors limites » et de *combiner* les ressources humaines et les moyens techniques, de « *ne plus penser et agir en silos*.[768] » Prenons la mesure du retard accumulé à travers l'analyse de Jean-Louis Gergorin :

> « *Il y a donc eu des changements majeurs en France, mais sur une position défensive ou contre-offensive, pas hégémonique ou offensive. Pour vous donner une idée, l'investissement dans les start-ups cyber en 2019 a été de quatre milliards de dollars aux États-Unis, d'un milliard pour Israël, de trois ou quatre cents millions au Royaume-Uni et de pas tout à fait cent millions pour la France et l'Allemagne réunies. Autrement dit, les Français et les Allemands investissent chacun un vingtième de ce qu'investissent les Israéliens dans les start-ups cyber. Ces écarts sont spectaculaires*. […] *Ceci illustre*

[766] https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php

[767] Stéphane Taillat, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Hérodote*, 2020/2-3 (n° 177-178), pp. 313-328, p. 313. Voir texte original : https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline.

[768] Comme le prônent les 54 experts (https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php).

*un problème fondamental : nous avons de l'argent, mais nous ne savons pas le dépenser efficacement*.[769] »

Ainsi, nous préconisons d'adopter une posture résolument offensive. En premier lieu, nous plaidons pour la constitution d'un état-major civil d'intelligence cyber, fondé sur une doctrine et une stratégie. Par conséquent, les principaux conseillers de cette structure seraient logiquement issus du monde du hacking et de la guerre informationnelle. La doctrine serait le fruit d'un travail conjoint à l'instar d'un rapport Martre ou Carayon pour le cyber, en fusionnant les travaux épars de ces dernières années issus de la réflexion des parlementaires et l'apport des meilleurs experts du domaine. La stratégie serait élaborée par un *coordonnateur national de l'intelligence cyber*, en lien avec l'idée émise par Bernard Barbier, Jean-Louis Gergorin et Édouard Guillaud[770]. L'idée d'un ministère du Numérique proposée en 2020 par les cinquante-quatre personnalités nous apparaît trop limitée et surtout difficile à mettre en place. Comment, en effet, un ministère à « vocation interministérielle » pourrait imposer une action transverse ?[771] Un état-major cyber piloté par un état-major d'intelligence économique nous paraît une proposition pertinente. Avant de développer cet axe d'une politique nationale d'intelligence cyber, nous proposons ce tableau récapitulatif des dispositions mentales à consacrer dans une approche combinée défensive et offensive.

| | |
|---|---|
| **Espace de référence** | Patrie, État-nation, territoires, pôles de compétitivité ; UE |
| **Réalités perçues** | Conflictualité omni-scalaire, pan-domaines et omnidirectionnelle |
| **Vision de l'économie** | Militaire/sécuritaire et compétition globale (champ de bataille) |
| **Grille d'analyse** | Géoéconomie et géostratégie du cyber, polémologie |
| **Valeurs** | Souveraineté numérique et intérêt national, cohésion sociale |
| **Culture stratégique** | Cyberoffensive et cyberdéfensive |
| **Posture stratégique** | Cyberpuissance, cyber-influence, cybersécurité |
| **Pratiques dominantes** | Cybersécurité offensive, contre-ingérence, cyber-renseignement, cyber-influence, sensibilisation, protection |
| **Prisme** | Géoéconomique, géostratégique et souverainiste |

**Figure 45 :** *Posture de cybersécurité offensive intégrant l'attaque et la défense combinées*[772]

[769] Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber…*, *op. cit.*, pp. 27, 31.
[770] Jean-Louis Gergorin & Léo Isaac-Dognin, *ibid.*, pp. 34-35.
[771] En effet, un ministère est par nature spécialisé, et l'ensemble des fonctions des affaires publiques thématiques que chacun exerce respectivement forme le gouvernement. Il ne paraît donc pas évident que lui revienne une charge interministérielle.
[772] Source : agrégation et reformulation des deux courants de l'IE (sécurité et guerre économiques) présentés par Franck Bulinge & Nicolas Moinet, « L'intelligence économique… », *op. cit*., p. 57 et p. 59.

### c) *Qu'est-ce que l'intelligence cyber ?*

On l'aura sans doute compris, ce que nous appelons l'intelligence cyber est une posture d'esprit et un dispositif opérationnel fondé sur une approche globale qui doit penser le cyber et y agir pour assurer un certain contrôle et une influence sur nos adversaires et nos alliés. Envisagée comme une fonction, l'intelligence cyber doit reposer sur une politique nationale et une structure stratégico-opérationnelle, diffuser un esprit critique du numérique, une culture du renseignement et de sécurité offensive qui traverserait toute la société. Cette politique inclusive d'éducation et de formation personnelles et professionnelles serait le socle du cyber et un outil d'employabilité et de souveraineté. Car cette approche nécessite au premier chef de garantir son autonomie techno-stratégique à notre pays.

## 3) L'impératif de souveraineté numérique

Comme le dit très justement Tariq Krim, pionnier du Web, entrepreneur et ancien vice-président du Conseil national du numérique :

> « *C'est l'Europe qui invente le Web, mais ce sont les États-Unis qui commercialiseront Netscape, le premier navigateur Web. Il ouvre la voie à la plus grande création de valeur de l'histoire de l'humanité. Linux, le moteur du Cloud, a été créé en Finlande, mais ce sont Google, Amazon et Facebook, Microsoft et les plateformes chinoises qui en profiteront vraiment. Face aux informaticiens et développeurs de la Silicon Valley, nous n'avions chez nous, aux manettes, que des politiques, des juristes ou des communicants. C'est la raison pour laquelle nous n'avons pas su faire émerger la filière logicielle que nous méritions. La plupart des politiques continuent d'ignorer que Linux, MySQL, Python, IRC, le Mpeg et le MP3, ainsi que bien d'autres briques fondamentales du Web moderne, ont été inventées en Europe, voire en France. C'est une des raisons pour lesquelles les investissements européens ont longtemps ignoré les créateurs de technologie Web et préféré financer de grands groupes qui n'ont jamais rien délivré. Une doctrine qui est toujours d'actualité.*[773] »

### a) *La souveraineté technologique en question*

Si certains boucliers ont été levés face à cette dépendance technique d'abord, à travers le RGPD et ses suppléments qui ne font toutefois que compenser notre faiblesse en termes de souveraineté sur la *datalocalisation*, notre degré de techno-sujétion est confondant. Quand Tariq Krim évoque le virage manqué par l'Europe et avance l'idée de sauver ce qui peut l'être par la résilience numérique, il prône en réalité un sursaut souverain qui permettrait au Vieux continent de frayer une « troisième voie numérique », celle de la neutralité. Entre l'avènement originel d'un internet ouvert puis son accaparement par quelques acteurs publics et surtout

[773] https://amp.lepoint.fr/2507586

privés, le risque d'un *Splinternet* se fait jour : la fragmentation et la militarisation du Réseau sont déjà à l'œuvre, annonçant un avenir assez sombre pour l'Europe. Chine et Russie en tête, trente-cinq États ont déjà commencé à découpler leur réseau national de l'Internet mondial, soit en exerçant une censure web fondée sur des résolveurs DNS « empoisonnés » ou sur la technique du *deep packet inspection* (DPI)[774], soit en bloquant simplement l'accès physique au réseau. Et étant donné que « *nous n'avons fait que louer, au sens propre et figuré les technologies issues de la Silicon Valley*.[775] », la situation risque de nous forcer à ne compter que sur les États-Unis et « *leur céder le contrôle opérationnel du principal moteur de notre croissance : un réseau Internet libre et ouvert*. » Rappelons du reste que sous le mandat de Donald Trump a précisément été votée la fin de la neutralité du réseau.

De fait, comme dans bien d'autres secteurs industriels où il est question de souveraineté et d'autonomie stratégique, l'Europe et la France se montrent tout à fait vulnérables. Or, on sait que les Américains vont sans vergogne exploiter nos faiblesses. Comme le déplore la hackeuse israélienne Keren Elazari, pourtant citoyenne d'une cyberpuissance, l'accès à l'information est une illusion car c'est un « *modèle féodal qui en contrôle l'accès et la nature. Aujourd'hui, les individus, même s'ils peuvent prendre une petite part potentielle de ce monopole, ne sont en fait que des sujets produisant pour des seigneurs. Des entreprises qui, à travers leurs algorithmes, remplacent les rois qui auparavant en avait la maitrise*.[776] »

C'est dès lors toute une société, européenne mais en particulier française pour ce qui nous occupe au premier chef qui s'est placée dans une situation de dépendance technologique préjudiciable à plusieurs titres. D'abord, notre absence de maîtrise sur les maillons de la chaine de valeur numérique est impressionnante. L'Europe n'a tiré aucun usufruit de ses propres inventions logicielles, l'amenant même à faire vendre à ses sociétés de services des outils que d'autres ont créés. Par exemple, même dans le domaine de la sécurité numérique, une bonne part des entreprises européennes vend localement des solutions qui sont en réalité américaines

[774] Le DNS *poisoning* est une technique d'attaque consistant à injecter des redirections de sites web à partir de requêtes usuelles sur un navigateur en usurpant les adresses IP pour diriger l'utilisateur vers des sites malveillants. Nous convoquons ici le nom de cette technique, même si un État filtrera simplement des adresses web (URL) non souhaitées au niveau des *résolveurs DNS*. Les résolveurs DNS permettent de convertir (*résoudre*) les noms de domaines (langage humain) en adresses IP (langage machine). Ils interviennent à la source de la navigation et peuvent donc filtrer des sites web qui ne seraient pas référencés dans les serveurs DNS. Les résolveurs DNS proposés par l'Union européenne permettent par exemple d'exclure des ressources considérées comme néfastes (https://www.dns0.eu/fr). Quant au DPI, c'est une technique d'inspection approfondie qui consiste à analyser en détail les flux de données et notamment les contenus des paquets (datagrammes), plutôt que simplement examiner leurs entêtes. Cela permet une censure plus efficace. Voir pour plus de précisions : https://openclassrooms.com/fr/courses/2340511-maitrisez-vos-applications-et-reseaux-tcp-ip/2927999-detaillez-len-tete-ip.

[775] Tribune de Tariq Krim, https://amp.lepoint.fr/2507586.

[776] Keren Elazari, Conférence TED, 10/06/2014.

ou israéliennes[777]. En outre, les produits logiciels notamment américains souffrent de failles logicielles importantes, car les entreprises qui les commercialisent pensent moins en termes de *security* – et bien sûr à dessein *privacy – by design* qu'en marchés à conquérir et solutions à écouler[778]. « Bob » évoque à cet égard la permanence de vulnérabilités informatiques : « *Il y a une "dette publique" à cause de la facilité en termes de programmation. Beaucoup de code est repris, par exemple Windows 10 ou 11 contient beaucoup de morceaux de code des anciennes versions.*[779] » En dehors même de l'aspect confidentialité et sans être parfait, le système d'exploitation Linux est connu pour être plus sécurisé par défaut que ses homologues américains privateurs.

Ensuite, il faut noter un deuxième maillon stratégique de notre chaine de souveraineté qui est en défaut face aux données personnelles et industrielles. Nous avons déjà évoqué plus avant les questions d'hébergement cloud et les problèmes que ce dernier posait quant à la confidentialité des données. Par exemple, Alibaba Cloud a été pressenti pour héberger les données liées à l'organisation des JO 2024. Finalement, même si la firme chinoise en sera bien chargée, c'est le Français Atos qui assurera l'hébergement des éléments les plus sensibles (autorités publiques, personnes accréditées, police…)[780]. Si ce type de signal envoyé est positif et dans le même temps toujours le fruit d'une réaction à une levée de boucliers, les autorités françaises sont tout de même moins regardantes lorsqu'il s'agit de sociétés américaines (ici, Cisco par exemple). Mais au-delà de ce qui peut apparaître comme relevant de questions techniques, il s'agit d'un véritable enjeu géopolitique, où l'influence des États se mesure à leur capacité à maitriser les technologies et normes qui sous-tendent l'industrie du numérique[781]. On sait par exemple que Pékin a placé un de ses citoyens à la tête de l'UIT (Union internationale des télécommunications), position enviable pour pousser telle nouvelle norme (« *New IP* ») ou tel ou standard comme la 5G chinoise – de Huawei –, en position de monopole mondial[782]. Toutes les technologies connexes à l'informatique font déjà l'objet d'une course sans merci : cryptographie, quantique, IA, nanoélectronique, blockchain, cyber-maritime, spatial…

[777] Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber…*, *op. cit.*, p. 42. Nous pouvons de notre côté attester que de l'aveu (ou désaveu) même des gendarmes, leur institution utilise certains outils israéliens à défaut de ressources domestiques.
[778] « Sécurité et confidentialité par conception ».
[779] Entretien avec l'auteur, 15/10/2021.
[780] https://www.lemonde.fr/sport/article/2022/09/23/jo-de-paris-2024-le-geant-chinois-alibaba-ne-s-occupera-pas-des-donnees-sensibles_6142932_3242.html
[781] https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php.
[782] Houlin Zhao a occupé le poste de secrétaire général de l'UIT durant huit ans (2015-2022), lequel représente un enjeu politique fort. La nouvelle secrétaire est une Américaine, élue face à un candidat russe. Le programme « nouvel IP » a été finalement rejeté au sein de l'agence : il aurait entravé la neutralité du réseau et vraisemblablement ouvert la voie à une plus grande censure de contenus Web (voir https://www.lemonde.fr/pixels/article/2022/09/29/l-americaine-doreen-bogdan-martin-elue-a-la-tete-de-l-agence-des-telecoms-de-l-onu-face-a-son-concurrent-russe_6143703_4408996.html).

Prenons l'analyse des *smart data* : on a évoqué précédemment le cas du Health Data Hub. En 2020, la spécialiste de l'IA Aurélie Jean pointait le mauvais signal envoyé par la France, dont le gouvernement avait justifié son choix de Microsoft pour des raisons platement techniques. Aurélie Jean expliquait alors que la souveraineté numérique est une affaire en réalité éminemment politique.

Enfin, au-delà des menaces d'ordre économique, cette dépendance technologique nous place face à un risque insoupçonné et pourtant tout à fait conséquent. Celui de la dilution de nos spécificités culturelles dans un imbroglio algorithmique où les puissances les plus avancées en IA vont façonner les esprits et favoriser, selon Tariq Krim, une « colonisation idéologique ». Il est notable qu'au même titre que les innovateurs de la Silicon Valley protègent leur progéniture des effets néfastes de leurs propres inventions, la Chine contrôle l'usage de son RSN vedette Douyin afin d'épargner ses jeunes ressortissants, tout en propulsant sans retenue sa version occidentale TikTok[783]. Le risque repose en définitive sur ce qui est déjà à l'œuvre, les RSN américains exerçant une influence déjà phénoménale rendant risibles les ancestrales techniques de *soft power* transatlantique. Pourrait-on arriver à une situation qui nous ferait perdre le contrôle de nos propres narratifs et valeurs européennes ? « *Il suffit déjà de voir comment les gigantesques bases d'apprentissage des nouveaux services d'intelligence artificielle de type ChatGPT produisent à travers leurs réponses les modes de pensée et les éléments de langage anglo-saxons*.[784] » Ainsi, la question mérite d'être posée. En bref, méfions-nous des « manipulateurs de symboles » que dénonçait Robert Reich dans son *Économie mondialisée*, et qui forment « *l'empire mondial* » du point de vue – ici biaisé – de Noah Yuval Harari, la caste des seuls bénéficiaires de la globalisation.

### b) *Quelle riposte ?*

La confiance numérique pose donc avant tout la question de notre souveraineté technologique. L'Europe ne manque pourtant pas de ressources industrielles et d'expertise académique, comme le mentionne le collectif des personnalités réclamant une stratégie numérique nationale. L'objectif consiste ainsi à s'appuyer sur ces moyens pour rendre la technologie européenne incontournable et à même de garantir une posture stratégique dans les situations d'interdépendance[785]. Est-il encore temps de créer une base industrielle technologique par le biais d'une infrastructure d'émancipation dotée de briques logicielles

[783] Sur le ton de la provocation, cet article de presse illustre ce possible stratagème de *sharp power* : https://www.lefigaro.fr/secteur/high-tech/comment-la-chine-protege-ses-enfants-et-rend-les-notres-debiles-avec-le-reseau-social-tiktok-20221214.
[784] https://amp.lepoint.fr/2507586.
[785] https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php.

souveraines ? Car, pour Tariq Krim, une bonne partie des startup françaises de cybersécurité privilégient le suivisme aux grandes plateformes américaines, quand leur financement n'alimente pas plus ou moins directement leur dépendance aux infrastructures techniques états-uniennes.

Encore une fois, l'Europe est à la croisée des chemins, et ce défi constitue tout autant une opportunité en vue d'établir une véritable voie de puissance d'équilibre. « *Face au principe de réalité,* explicite Tariq Krim, *la véritable bataille est idéologique. Les dirigeants européens et français n'ont ni vision ni volonté politique. La peur de l'inconnu les paralyse*. » Mais plusieurs voies se dessinent, si les politiques acceptent enfin d'écouter les développeurs – européens – des technologies de l'Internet : *edge computing* (IA à faible coût de calcul), logiciels émancipateurs, cryptographie quantique… Avec son initiative « Semi-conducteurs pour l'Europe »[786] et l'objectif d'atteindre 20% de part du marché mondial d'ici à 2030, l'UE semble avoir fait un pas dans la prise de conscience de sa vulnérabilité. Gageons qu'elle fasse de même sur d'autres secteurs de l'informatique et du numérique, ceux où il est encore temps de se placer entre l'enclume chinoise et le marteau américain. « *Les munitions techniques sont à notre disposition. Saurons-nous les utiliser ?* [787] »

Si la souveraineté numérique et donc technologique constitue la première brique de notre émancipation, il revient à la France de mieux se protéger face à la cybermenace polymorphe. Se passer des hackers ou les utiliser *a fortiori* sans objectif clair ne nous serait que préjudiciable. En revanche, les incorporer dans un dispositif orienté par une stratégie de cybersécurité offensive peut sans nul doute nous aider à relever le défi.

[786] https://www.consilium.europa.eu/fr/policies/eu-industrial-policy/eu-chips-industry/
[787] https://amp.lepoint.fr/2507586.

## **B.** *Intégrer les hackers dans une stratégie de cybersécurité offensive*

> « *Nous avons besoin de tous les hackers possible, de gens qui dialoguent avec le monde numérique. Pas juste en l'utilisant comme nous y incitent les entreprises féodales*. […] *Je pense que les hackers ont un pouvoir transformationnel.* »
>
> Keren Elazari

Sécurité, vie privée et souveraineté font bon ménage. Au centre de la triade, l'identité numérique est le nerf de la confiance numérique. « *Nous disposons de tous les atouts industriels et d'une excellence reconnue dans plusieurs domaines essentiels pour faire entrer notre pays dans un cyberespace maîtrisé. Dans cet espace, une vision holistique de la confiance numérique nous permettra de faire valoir nos valeurs et notre souveraineté, et de les défendre*.[788] » Au carrefour entre les deux murs porteurs de cet édifice, les hackers pourraient bien en représenter la clé de voûte. En lien avec l'équipe des bleus, l'équipe des rouges peut s'avérer des plus agile pour marquer l'essai que leur doivent les politiques de notre pays. Blancs au centre. Ainsi, donner leur chance aux hackers éthiques qui sont en effet les mieux placés pour assurer cette combinaison des moyens, des ressources et des savoir-faire. Qui de mieux placés pour assurer la sécurité de nos systèmes d'information ? Mais la réalité, loin d'être manichéenne, est souvent grise, comme le sont ces hacktivistes qui n'ont pas forcément tous des intérêts divergents de ceux des autorités et peuvent ainsi jouer collectif au service de notre cohésion. La cybersécurité est une chaine où tout maillon faible joue malheureusement contre son camp. Elle est en vérité l'affaire de tous.

Et réclame donc toutes les attentions, auxquelles une véritable politique nationale d'intelligence cyber peut pourvoir dans le cadre d'une vision stratégique. L'éducation en constitue la pierre angulaire, tant pour la formation spécialisée qu'elle doit apporter aux professionnels d'un marché lacunaire à combler, que pour l'infusion d'une culture qui s'acquiert comme chacun sait dès le plus jeune âge. C'est ce fil conducteur d'une posture de sécurité qui doit traverser les *cursus honorum* scolaires à universitaires des citoyens français. D'un point de vue organisationnel, cette politique vise la création d'un dispositif intelligent de cybersécurité offensive et la mise en place d'une instance de dialogue entre les hackers français et leur État. L'ensemble du système, enfin, se doit de placer les hackers parmi les acteurs opérationnels comme maîtres des jeux du cyber-renseignement fermé et ouvert, de la sécurité informatique et de la cyber-influence.

[788] https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php

### 1) Penser et déployer une politique nationale d'intelligence cyber

Quatre briques fondamentales sont envisagées pour l'édification d'une politique d'intelligence cyber : la pierre de l'éducation ; celle d'une interface hackers-État ; puis, un dispositif intelligent noyauté par des hackers sélectionnés et des profils polyvalents, entre compétence technique et savoir contextuel. Enfin, ce dispositif serait piloté par un coordonnateur au sein d'un état-major chargé d'articuler les trois fonctions suivantes : renseignement-anticipation (OSINT), cybersécurité offensive et cyber-influence. Cet état-major cyber opérationnel viendrait se greffer réticulairement à un grand état-major d'intelligence stratégique tous deux à vocation transversale et dans une logique de subsidiarité. Objectif : créer des synergies et un environnement symbiotique à travers une politique intégrée.

#### a) *Le volet éducation-formation*

« *Work like a spy*. » Tel est le titre de l'ouvrage d'une ancienne cadre d'entreprise reconvertie en officière de la CIA[789]. Entre maîtrise du profiling psychologique et des *soft skills*, habileté au réseautage, élicitation et posture de sûreté permanente, J.C Carleson narre son parcours hors du commun et pourtant très terre-à-terre lorsqu'il s'agit d'exposer les avantages à tirer de cette expérience si elle était appliquée au monde civil et économique. C'est cette posture-là qui doit définir l'approche éducative de notre pays. Ainsi, former des citoyens éclairés à plusieurs niveaux. Le premier concerne sans nul doute l'absence de véritable culture de critique des médias numériques et sociaux comme l'a d'ailleurs fait entendre David Colon[790]. À côté des initiatives personnelles de certains enseignants, aucune formation sérieuse n'a été mise au programme de l'enseignement secondaire. Or, les générations actuelles souffrent d'un cruel manque de recul face au pouvoir et à la banalisation de l'image, dont les dérives liées aux RSN sont les plus funestes illustrations. L'État doit donc prendre toute sa part de responsabilité et permettre l'éducation au numérique et à ses dangers d'ordre cognitif.

Au-delà de cet aspect fondamental, la formation initiale et continue à tous les âges est un point cardinal à développer pour deux raisons : d'abord, l'employabilité dans un secteur en croissance continue car indexée sur la numérisation permanente. Qu'il s'agisse du secteur du numérique et des nouvelles technologies, l'importance d'apprendre à coder est prégnante. Évidemment, le secteur de la sécurité informatique nécessite d'énormes ressources humaines, face à une pénurie mondiale estimée à 3,5M et qui de surcroît se creuse[791]. En Europe, ce chiffre

[789] J.C. Carleson, *Work Like a Spy: Business Tips from a Former CIA Officer*, Portfolio, 2013, 208 p.
[790] David Colon, *La guerre de l'information : Les États à la conquête de nos esprits*, Tallandier, 2023, 480 p.
[791] https://www.forbes.com/sites/forbestechcouncil/2023/01/25/better-management-and-training-are-key-to-solving-the-cybersecurity-skills-gap/

est estimé à 350 000 spécialistes et en France, entre 15 et 20 000, l'ANSSI parlant de 75% des besoins non pourvus dans nos entreprises[792]. Or, ce n'est qu'en février 2023 que l'État a décidé de traiter le sujet avec un programme d'investissement de 1M€, pour l'enseignement supérieur[793]. Par ailleurs, on sait que la filière n'attire pas les étudiants. Sur ce point, plusieurs hackers se sont manifestés, à l'instar de Victor Poucheret et Brice Augras. Ils déplorent en effet les « programmes scolaires pauvres » et « le manque de formation », évoquant leur intervention dans certaines écoles. Ils disent avoir reçu une trame de programme venant du ministère de l'Éducation nationale dont les contenus n'étaient pas à jour à hauteur de 80%. En outre, ils parlent d'une approche trop théorique basée sur des aspects normatifs et juridiques peu attrayants, et prônent le changement des méthodes d'apprentissage et plus de flexibilité. En tant qu'enseignant, nous avons déjà évoqué la disparité des contenus de formation entre écoles d'informatique, l'absence de cours d'OSINT ou de vrais modules denses sur le *pentesting*, la rétro-ingénierie ou la forensique[794].

En second lieu, intervient donc la spécificité des formations du supérieur. Selon Julien Métayer, aucun établissement ne propose de cursus purement axé sur la cybersécurité et *a fortiori* sur le domaine du hacking. Il s'agit plutôt de briques de spécialité rattachées à un tronc commun du type administrateur réseau/système. Tout est tourné, poursuit-il, vers le défensif. Les offres (souvent des licences spécialisées) commencent toutefois à apparaître[795]. Selon Damien Cazenave, les RSSI sont rarement dotés d'un esprit offensif, souvent pour des raisons de tempérament, de manque de temps, de finance ou de formation[796]. D'une manière plus générale, pour être force de propositions de formation aux bases de la SSI, nous constatons que les écoles de l'enseignement supérieur ne s'intéressent que trop peu aux questions de sécurité. Si certains responsables pédagogiques se montrent beaucoup plus réceptifs et conscients de l'importance de ces sujets, leur direction ne leur permet que rarement d'y répondre, soit par manque de temps de programmation soit par désintérêt.

En somme, c'est d'une vraie culture du renseignement et de la sécurité que le pays a besoin. De vraies communautés existent en France et se distinguent par leur savoir-faire, entre les communautés de hackers à proprement parler et celle des OSINTers, propulsée par des journalistes d'investigation, des chercheurs académiques, des experts en cybersécurité ou

[792] https://www.challenges.fr/emploi/formation/cybersecurite-ces-initiatives-pour-repondre-a-la-penurie-de-talents_831542 ; https://www.francetvinfo.fr/replay-radio/c-est-mon-boulot/emploi-les-specialistes-de-la-cybersecurite-de-plus-en-plus-demandes_4950486.html

[793] https://www.lemonde.fr/campus/article/2023/04/17/l-enseignement-superieur-en-ordre-de-bataille-pour-contrer-la-penurie-de-talents-dans-la-cybersecurite_6169868_4401467.html

[794] Bien souvent, l'ingénierie pédagogique fait défaut et certains établissements s'en remettent même aux intervenants – de moins en moins nombreux compte tenu de leur faible valorisation – pour élaborer leurs contenus de programmes.

[795] Entretien avec l'auteur, 30/03/2022.

[796] Entretien avec l'auteur, 24/07/2017.

certains hackers. Plusieurs initiatives sont à mettre en avant comme la plateforme d'auto-apprentissage *ozint.eu* fondée par Julien Métayer, la communauté *osintfr.com* et l'association *openfacto*. C'est par ces voies-là probablement que l'intérêt grandira autour de la cybersécurité, du hacking et de l'investigation numérique, domaines tous trois interdépendants. Certains producteurs de contenus de réseaux socionumériques, comme Michaël de Marliave *alias* « Micode », peuvent pareillement constituer des passerelles intéressantes à l'adresse des jeunes générations, en vulgarisant efficacement des sujets souvent ardus. Néanmoins, former des spécialistes et démocratiser ces domaines ne peut suffire à diffuser une culture stratégique. Il faut pour ce faire établir un maillon de confiance entre les autorités étatiques et les hackers.

### b) *Créer une interface de dialogue entre autorités et hackers*

En dépit des avancées législatives mais perfectibles réalisées dans la prise en compte des hackers dits éthiques, de l'émergence de plateformes désormais reconnues pour la mise en relation des hackers avec les entreprises encadrant les pratiques du *bug bounty*, peut-on pour autant parler de structuration formelle d'une communauté de hackers en France ? Quelle est, de fait, la part de représentation et de représentativité des hackers ? Pour Yassir Kazar, fondateur de Yogosha, il manque bien un organisme pouvant former le porte-voix de ces derniers. Et de citer le Chaos Computer Club comme modèle naturel, « *qui a réussi à s'imposer comme tel, un vrai interlocuteur face à l'État allemand*.[797] » Selon lui, il revient aux hackers français de prendre les devants et de créer une telle structure. Mais il manque une assise politique et un leadership qui porterait de vraies revendications. Cela s'explique-t-il par la défiance nourrie de longue date de la part des hackers français ? Ou ces derniers souffriraient-ils du même mal individualiste que leurs compatriotes hexagonaux ? En tout état de cause, l'initiative pourrait-elle venir du Parti pirate (PP), certes bien plus influent et visible dans les pays nordiques dont il s'est inspiré ? Ou bien dans un alliage entre La Quadrature du Net, HackerzVoice et Hackers sans frontières ? Guillaume Poupard rejoint Yassir Kazar et cite HackerzVoice, l'association organisatrice de *Le Hack*[798]. Une telle structure est nécessaire car selon Fabrice Epelboin, l'État n'est en contact qu'avec des individus et non un groupe officiel. Pierre Penalba, de son côté, explique que si l'histoire entre le Chaos Computer Club et les autorités allemandes n'a pas toujours été simple, celui-ci a néanmoins réussi à s'imposer comme une interface qui discute avec l'État.

Au bilan, cette instance de dialogue ne pourrait être que bénéfique pour instaurer une confiance mutuelle et identifier clairement les hackers les plus investis et donc les plus

[797] Entretien avec l'auteur, 20/05/2022.
[798] Entretien avec l'auteur, 17/04/2023.

patriotes. Ce faisant, ces profils pourraient composer le noyau dur d'un dispositif synergique, où spécialistes de la guerre informationnelle et hackers structureraient l'attaque, et experts en SSI et spécialistes IE et RI organiseraient la défense.

### c) *Mettre en place un dispositif intelligent piloté par un état-major cyber*

Au même titre qu'un CNRLT[799] permet d'assurer une certaine harmonie et cohérence entre les différents services de renseignement, la politique d'intelligence cyber s'articulerait sur un coordonnateur en charge de la combinaison des moyens qui élaborerait la vision stratégique du cyber. Lui reviendrait le soin de mettre en synergie les différentes fonctions intégrées dans le cadre d'un état-major dédié, à savoir une brique renseignement sur la menace (CTI)/OSINT ; une deuxième sur la cybersécurité offensive ; une dernière sur la cyberinfluence/contre-influence – qui pourrait opportunément intégrer Viginum, la sortir de sa condition d'isolat organisationnel et lui offrir plus de moyens humains et financiers[800]. Le COMCYBER resterait sous la tutelle du MINARM et l'ANSSI sous celle du SGDSN en restant à compétence interministérielle et chargée de la SSI des ministères (hors MINARM, donc sans attributions de cyberdéfense). En outre, des synergies seraient favorisées avec les entreprises nationales via l'intermédiaire de sociétés d'économie numérique, sorte de *sōgō shōsha cyber*. Très globalement, cette vision – au stade exploratoire – peut être illustrée par le schéma suivant :

[799] Coordonnateur national du renseignement et de lutte antiterroriste.

[800] Viginum est le service de vigilance et protection contre les ingérences numériques étrangères (https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques).

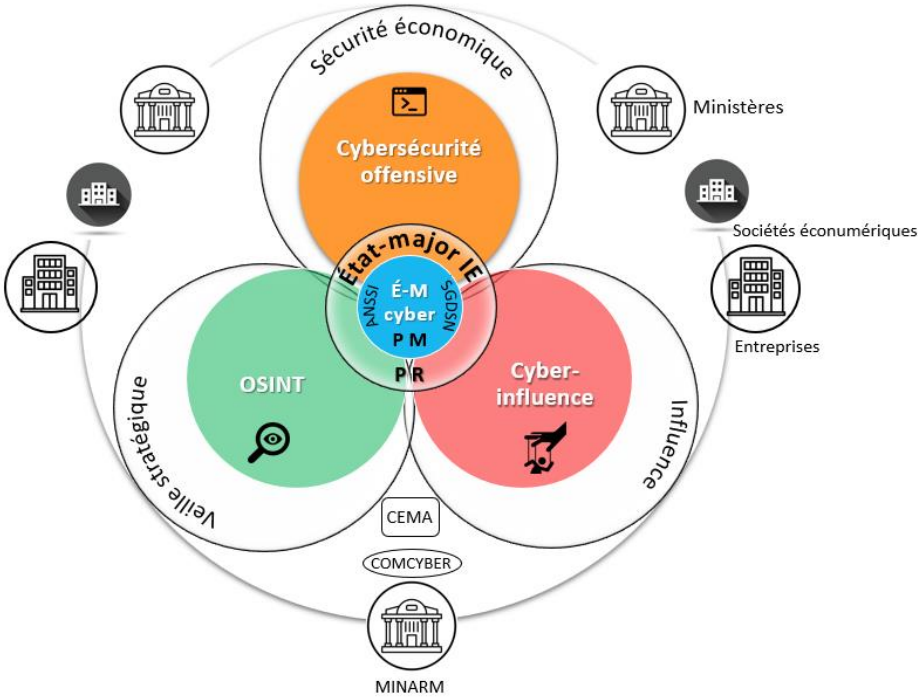



**Figure 46 :** *Vision d'un état-major d'intelligence cyber, enchâssé dans un état-major IE*

Légende – PR : l'état-major d'intelligence économique est placé sous l'autorité du Président de la République ; l'état-major d'intelligence cyber sous celle du Premier ministre (PM).

La composition de l'état-major d'intelligence cyber devrait être composé de différents profils, ce qui nous ramène aux questions de l'éducation-formation et de culture stratégique. Ainsi, les postes primaires *techniques* de haut niveau en *sécurité offensive* seraient confiés à des hackers (*rouges*) sélectionnés selon les critères du renseignement (SANSOUCIS[801]) tandis que la *sécurité défensive* serait assignée à des profils (*bleus*) de type RSSI. Les postes secondaires *analytiques* seraient dédiés à des chercheurs/universitaires en sciences humaines et sociales : pour schématiser, des spécialistes en géopolitique, géoéconomie, et psychosociologie. Leur tâche consisterait à apporter contexte et analyse aux évènements en transmettant leur savoir aux « sachant-faire » (les techniciens). Sachants et sachant-faire pourraient opportunément et par fertilisation croisée enrichir leurs connaissances générales. Frédérick Douzet explique que des profils SHS[802] aident à la contextualisation en matière de représentations géopolitiques, évoquant une certaine hybridation[803]. De son côté, Christian

[801] L'acronyme SANSOUCIS (ou l'équivalent anglosaxon MICE : *Money, ideology, constraint, ego*) est mis pour « solitude, argent, nouveauté, sexe, orgueil, utilité, contrainte, idéologie, suffisance ». Il sert de base méthodologique au recrutement ou à la manipulation de sources humaines. Inspiré du MICE anglais, il aurait été inventé par la DST.

[802] Sciences humaines et sociales.

[803] Entretien avec l'autrice, 30/03/2022. Elle acquiesce quand nous lui parlons de la CTI.

Harbulot évoque lors de notre entretien une anecdote éclairante. Favorisant l'interdisciplinarité et dans le cadre d'un exercice commun, l'École de guerre économique met en lien ses étudiants avec ceux d'une école d'informatique. Ils travaillent alors de concert sur des études de cas. Or, il était ressorti que les *techniciens* avaient parfois du mal à appréhender certaines données situationnelles (par exemple, bien appréhender le facteur humain dans les attaques d'ingénierie sociale – *phishing*). Leur cadre technique les plaçait dans des biais de cadrage auxquels les étudiants en IE, avec leur regard déporté, étaient moins soumis. En ce qui nous concerne, l'approche « sociotechnique » de la cybersécurité que nous enseignons à des étudiants en informatique les sort du cadre classique, souvent normatif, juridique ou à l'inverse trop orienté vers la technique pure. En décentrant le regard, ils peuvent enrichir leur formation pour limiter l'effet tunnel. C'est pourquoi le croisement de différentes approches ne peut qu'être bénéfique, soutenant par là même une dynamique d'intelligence collective.

Au-delà de ce qui semble toutefois demeurer une forme de dichotomie, nous voyons une voie médiane. Si les deux types de profils, analytiques d'un côté et techniques de l'autre, peuvent représenter en quelque sorte la tête et les bras, il semble néanmoins de plus en plus utile de disposer de « spécialistes polyvalents » ou de multispécialistes pourrait-on dire. Encore une fois : il s'agit de décloisonner les savoirs comme ne le renierait pas un Edgar Morin. Nous sommes ainsi convaincu qu'il faut revenir à un certain degré de polyvalence sans forcément atteindre le plus haut degré de polymathie à l'instar des Lumières. Ainsi, posséder des compétences techniques, en programmation et dans une spécialité du hacking : *pentesting*, rétro-ingénierie, forensique… par ailleurs OSINT ; et des compétences en SHS dont une ou deux spécialités (RI+IE, IE+sociologie…)[804]. Se poser à la fois en sachant et sachant-faire. Pour une raison au moins : comprendre et savoir écouter le collègue technicien ou analyste. Communiquer. Dans cette optique, la CTI est l'exemple d'une certaine polyvalence, même si les postes peuvent être encore séparés. Cette discipline allie les compétences en géopolitique avec celles de l'informatique et de l'OSINT[805]. L'OSINT est d'ailleurs à la croisée des chemins, car posséder un savoir technique permet d'améliorer ses aptitudes dans l'investigation numérique. Le schéma ci-dessous éclaire les aspects techniques et analytiques qui se croisent dans la CTI.

[804] Sans les citer, certains profils – encore rares – ont par exemple combiné une formation en sécurité informatique et un cursus en SHS. Nous-même, modestement. Les reconversions professionnelles, plus nombreuses aujourd'hui permettent indirectement de croiser des expériences différentes mais quasi-toujours complémentaires.

[805] Nous connaissons certains profils issus des Relations internationales n'ayant aucune compétence technique mais travaillant dans la CTI. Il faut bien sûr nourrir une appétence pour le domaine, mais on apprend peu à peu la technique au contact des informaticiens spécialisés.

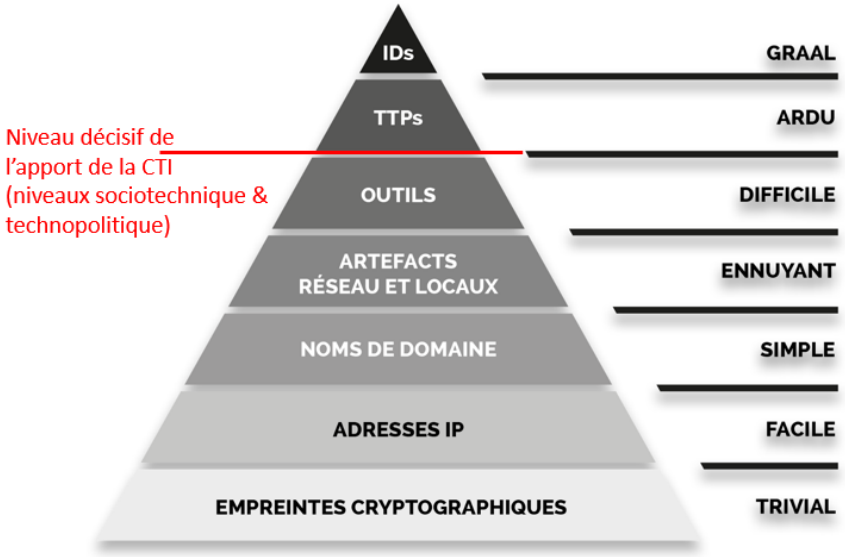



**Figure 47 :** *« Pyramide de la cyber-douleur » par David J. Bianco/Sekōia*[806]

Schéma modifié par la société de cybersécurité française *Sekōia* (ajout des « IDs », à savoir l'identité des attaquants) et par nous-même (ajout en rouge). Voir la source pour plus de détails.

Cette pyramide symbolise l'activité de la CTI. Elle décrit comment « faire mal » aux cyber-agresseurs, en collectant des preuves numériques en quête de l'attribution technique/juridique voire de l'imputation politique des attaques. Il s'agit de prélever tous les items de la pyramide pour remonter à la source. Évidemment, c'est d'abord la victime « qui souffre », mais la CTI repose sur l'idée au moins symbolique de ne pas laisser le crime impuni et de mieux anticiper les futures agressions.

S'agissant de l'aspect culturel enfin, il est nécessairement lié à cette question de l'éduction-formation et au monde entrepreneurial. Autrement dit, la stratégie de l'état-major cyber et celle des entreprises privées doivent s'irriguer mutuellement. Le point de vue de Jean-Louis Gergorin nous éclaire une nouvelle fois. Pour lui, il y a un réel problème culturel en Europe et en France, où la vision de l'innovation et du développement reste très colbertiste. Caractérisée par les grands programmes, elle ne semble pas s'adapter facilement à l'économie du numérique qui requiert, selon lui, une approche totalement différente et prenant pour exemple la Chine ou Israël et ses startups[807]. En effet, on sait que les réseaux qui maillent les SR et le monde économique sont très denses là-bas comme aux EUA du reste. L'unité 8.200 de Tsahal notamment a construit un véritable écosystème autour d'elle et accouche de nombreuses sociétés de cybersécurité et de renseignement privé. Or, comment procède-t-elle ?

[806] https://medium.com/cyberthreatintel/the-pyramid-of-pain-ou-l%C3%A9chelle-de-la-cyber-douleur-47b75201f02f
[807] Jean-Louis Gergorin & Léo Isaac-Dognin, *Cyber…*, *op. cit.*, p. 41.

Selon Jean-Louis Gergorin, dès le secondaire le système éducatif sélectionne les plus doués en mathématiques et en hacking. Plus tard, après leur service national obligatoire, les jeunes Israéliens sont encouragés à rejoindre ou créer leur propre entreprise dans le numérique. Plus proche de nous, le Royaume-Uni a adopté et adapté ce modèle en lien avec le GCHQ, dont le général Gomart vante d'ailleurs les mérites et évoque le souhait de voir un tel service être établi en France[808]. Ainsi, le GCHQ a engendré la firme Darktrace, l'un des leaders de l'IA appliquée à la cybersécurité.

Si la France suit par mimétisme ce même chemin avec notamment le fleuron TEHTRIS, fondé par deux anciens officiers de la DGSE, Éléna Poincet et Laurent Oudot, notre pays doit opérer une véritable révolution culturelle. Ancien hacker français très respecté, ce dernier est à l'image de la voie à suivre et à dépasser : intégrer pleinement ces profils dans le dispositif national.

### **2)** Les hackers comme atout maître du dispositif d'intelligence cyber : OSINT, cybersécurité offensive, cyber-influence

*« Comme les gentilles bactéries dans notre système immunitaire, on est des centaines voire des milliers mais, comme chaque bactérie, on travaille différemment. Il y a plusieurs types de hackers qui travaillent individuellement, ils ne sont pas connectés mais ils ont tous un impact sur nous parce qu'ils découvrent et rapportent des vulnérabilités. Et même les hackers malveillants, les cybercriminels, nous aident en nous faisant évoluer et nous forcent à remarquer les problèmes et créer quelque chose de meilleur auprès des entreprises qui créent les technologies. »*

Keren Elazari

Les hackers français sont-ils ne serait-ce qu'inclus dans notre organisation souveraine ? C'est la question posée depuis le début de notre travail. Si l'on en croit Brice Augras, la réponse semble mitigée : « *À l'heure actuelle, il y a un peu une étanchéité entre la communauté – mais ça ne veut pas dire que ça représente tout le monde – et nos autorités compétentes en France, le MINARM, etc. C'est assez deux mondes à part. On se concentre plus sur l'engagement citoyen. Aller aider la Croix-Rouge par exemple.* » Son compère Victor Poucheret poursuit et pose une question pertinente : « *Admettons, demain, que toute la communauté du pays soit fédérée vis-à-vis des actions de cyberguerre. Concrètement, ça se passe comment ?* [809] » Et de citer les principaux problèmes que cela soulèverait : les attributions d'attaques, l'engagement de civils, et plus trivialement la question de l'adaptation au monde militaire pour des

[808] Entretien avec l'auteur, 23/08/2017. Selon lui, la France manque d'un service équivalent à la NSA/au GCHQ.
[809] Interview de Brice Augras et Victor Poucheret, chaine *Thinkerview*, *op. cit*.

indépendants comme eux. Pour eux, ça concerne la cyberdéfense. On a déjà cité leur expérience malheureuse avec la Réserve opérationnelle/citoyenne de cyberdéfense. Pourtant donc, la volonté d'apporter leur aide est manifeste.

Précisément, n'est-ce pas le cœur du problème ? En d'autres termes, pourquoi cette communication ne se fait-elle pas ? Cela se peut-il du reste, dès lors qu'aucune vraie structure de dialogue ne le permet de manière cadrée, officielle et rassurante pour chacun ? C'est bien de notre dispositif intelligent qu'il s'agit. Aussi, en vertu de notre politique nationale, un état-major d'intelligence cyber doit être créé. Il coordonnerait alors les trois volets suivants : OSINT, cybersécurité offensive et cyber-influence.

#### a) *Cyber-influence et infoguerre : jouer aux intersections*

Comme l'explique très justement Nicolas Curien, le cyberspace « *apparaît* [...] *comme une prothèse de notre cerveau* [...] *plus exactement, comme une prolongation collective et partagée de l'ensemble des cerveaux humains, littéralement une "noosphère" ou sphère des esprits*.[810] » Dans le cyberespace, on peut associer les notions de *hard*, *soft* et *smart power* respectivement aux couches physique (géopolitique et géoéconomie des câbles...), logique (plateformes et services numériques, « *le médium est le message*[811] »), et socio-cognitive (l'influence par l'information et le savoir). Il est convenu de dire que les États-Unis maîtrisent une bonne partie de ces « structures de pouvoir » désormais associées *ipso facto* au cyber. Parmi ces lignes de force définies par Susan Strange[812], celle de la communication et du savoir. Or, la guerre de l'information s'insère dans cette structure à tous les niveaux : politico-militaire, médiatique, socioéconomique. Elle devient un enjeu crucial car elle aussi prend une dimension inégalée avec l'écho que lui confère le cyberspace. Au même titre qu'une attaque par rebond, cette lutte d'influence infocommunicationnelle se fait par l'intermédiaire de relais conscients ou pas. L'*astroturfing*, notamment, consiste à faire passer pour neutre de l'information en réalité sponsorisée (propagande, publicité), en s'appuyant sur des campagnes de désinformation destinées à générer des mouvements massifs d'opinion. Plus généralement, le risque est que l'information devienne simplement de la communication. Là où des pays comme la Russie (avec ses « usines à trolls » et son Ru.net), les États-Unis (avec leurs *spin doctors* et leur *soft power*) ou la Chine (et sa « *water army* »[813]) ont concentré leurs forces – humaines

[810] Nicolas Curien, « Inventer ensemble notre futur numérique : une ardente obligation ! », *Prospective et Stratégie*, n°9, 2018/1, pp. 23-35.
[811] Herbert M. McLuhan, *La Galaxie Gutenberg*, Biblis, 2017, 552 p.
[812] Susan Strange, *Le retrait de l'État : la dispersion du pouvoir dans l'économie mondiale*, Temps présent, 2011, 352 p.
[813] Le Ru.net ou Runet est l'ensemble des applications techniques et sémantiques du cyberespace russe. Les « usines à trolls » russes forment l'officielle organisation IRA (*Internet Research Agency*), créée par feu Evgueni Prigojine à Saint-Pétersbourg. La Water Army est son équivalent chinois.

et algorithmiques – dans l'espace cognitif, la France est restée longtemps inactive et a privilégié les aspects techniques du combat numérique. On l'a dit, ce n'est qu'en 2021 qu'une doctrine de lutte informatique d'influence (L2I) est formalisée et seulement en 2022 que l'influence est érigée en fonction stratégique.

Pourtant, c'est sur la couche sémantique que se joue précisément cette lutte d'influence, cette « infoguerre ». Fin 2018, l'Appel mondial pour la cybersécurité – focalisé sur les aspects de désinformation ou la question du *hack back* pour les acteurs privés – lancé par le président français fait figure de prise de conscience. Mais la contre-influence reste une posture défensive et réactive, et le cyberspace se prête mal aux incitations normatives à l'adresse d'une conflictualité *de facto* indirecte et opportuniste. L'usage d'une extraterritorialité juridictionnelle par les États-Unis, en particulier à des fins économiques, montre clairement que le droit lui-même peut être instrumentalisé dans le cadre de la guerre cognitive. Comme le disait assez justement Edward Bernays, « *la meilleure défense contre la propagande, c'est plus de propagande.* » En définitive, dans ce *brouillard informationnel*[814] l'influence est partout, à cheval entre diplomatie, *PsyOps*, propagande, publicité, communication, lobbying et *nudge*. Dans le privé, chez les ONG militantes, l'euphémisme est saisissant : on fait du « plaidoyer » ; ainsi du poste de « chargé de plaidoyer » au sein de leur organigramme. Le lobbying, version non lucrative. À partir d'une terminologie juridique, en effet, comment mieux exprimer la légitimité d'une cause ? Telle est la logique de l'influence : jouer des symboles et des perceptions dans une réalité où la rationalité trouve ses limites.

Que peuvent donc apporter les hackers dans la cyber-influence ? Probablement leur connaissance des ressorts techniques derrière les pratiques de manipulations de grande envergure en particulier par le biais de l'IA et des dernières technologies numériques. Par ailleurs, comme le dit Keren Elazari, le hacker peut être un « tricheur », y compris le plus honnête d'entre eux, « *quelqu'un d'assez intelligent pour jouer des tours aux gens. C'est une autre facette de l'état d'esprit du hacker.* » Autrement dit, ils ont des aptitudes à l'intelligence rusée et relationnelle. Ils sont donc bien souvent maîtres dans l'art de l'ingénierie sociale. Ainsi, à l'image du HUMINT, le cyber-HUMINT, sorte de *renseignement humain augmenté*, représente un nouvel enjeu[815].

Méconnue, cette notion a été théorisée en 2014 par un universitaire bulgare (Sofia), Amit Steinhart. Dans un court article[816] publié de manière plutôt confidentielle, celui-ci appelle en premier lieu à revenir aux fondamentaux du renseignement, où le facteur humain reste

[814] David Shenk, *Data Smog: Surviving the Information Glut*, HarperOne, 1997, 256 p.
[815] Terry Zimmer, *Le renseignement humain à l'ère numérique*, VA, 2018, 200 p.
[816] https://www.academia.edu/8457596/The_future_is_behind_us_The_human_factor_in_cyber_intelligence_Correlations_between_Cyber-HUMINT_and_Hackers_Social_Engineering.

essentiel en dépit de la révolution du numérique. Puis il dresse, en second lieu, un parallèle entre ingénierie sociale et HUMINT, constatant qu'on les amalgame parfois, en arguant que les deux sont également efficaces en fonction des situations et des cibles visées. Il conclue donc sur l'utilité de joindre les deux en un cyber-HUMINT qui doit être enseigné notamment aux jeunes professionnels de la cybersécurité. Très juste dans le constat sur l'aveuglement technologique, cette analyse oublie toutefois que « l'ingénierie sociale » n'a pas attendu l'avènement du cyber pour préexister à la dénomination. Par ailleurs, elle sépare la pratique de l'ingénierie sociale relative aux hackers d'un côté, et le renseignement humain des services d'État de l'autre. Nous pensons que cette dichotomie est artificielle, précisément car l'ingénierie sociale ou *élicitation* n'est qu'un sous-produit du HUMINT fondé lui aussi largement sur la manipulation, la duperie et le contrôle. En fin de compte, ces deux pratiques se conjuguent et trouvent écho dans les éléments de doctrine française sur le renseignement humain (ROHUM)[817] : le ROHUM-C se traduirait donc en « ROHUMOC », *renseignement humain d'origine cyber* ; le ROHUM-R en « ROHUMIC », *renseignement humain d'intérêt cyber*. En somme, le cyber-HUMINT recouvre plus que de l'humain à travers du technique : il est du renseignement socio-technique. À la fois parce qu'il se sert de dispositifs *physico-logiques* sur lesquels l'humain va investiguer (ROHUM-Reconnaissance), et par ce qu'il est une simple extension du renseignement humain (ROHUM-Conversationnel), l'exploitation d'êtres *psycho-logiques*. Le renseignement humain passe en effet par l'infiltration – sous couverture – de milieux dont on veut obtenir des informations. Appliqué au cyberespace, où la « conversation » est une interaction indirecte non physique, il fait surgir des problématiques nouvelles telles que l'anonymat/pseudonymat et les identités multiples ubiquitaires (« avatars », de véritables « légendes »).

Bien entendu, des profils plus analytiques ou experts en guerre de l'information sont parfaitement bien placés pour suppléer ou assister les hackers dans le domaine de l'influence. Ces derniers restent toutefois d'excellents candidats, notamment ceux qui ont un passé de *black hat* (du type Florent Curtet) ou font partie des hacktivistes. Leurs pratique concrète et expérience dans *l'art de la supercherie* ne peut en effet que les prédisposer au mieux à ces activités. Mais les hackers sont avant toute chose des experts techniques de la sécurité informatique.

### b) *Généraliser la cybersécurité d'approche offensive*

Dans la très vaste majorité des cas, la cybersécurité est appréhendée selon un angle défensif. C'est ce qui vient le premier à l'esprit des autorités étatiques, entreprises ou simples citoyens. Cet état de fait peut paraître évident car, qu'il s'agisse de sûreté ou de sécurité à

[817] La doctrine française distingue le ROHUM-Conversationnel et le ROHUM-Reconnaissance.

proprement parler, l'on considère qu'il faut se protéger d'une menace. Bien évidemment, au même titre que l'expression de défense est un euphémisme comme dans le cas de l'ancienne appellation du MINARM (« ministère de la Défense »), alors qu'il était désigné du nom de « ministère de la Guerre » jusqu'en 1940, le terme de sécurité édulcore la dimension réelle du concept. Or, notre pays n'a jamais eu à se défendre contre une agression et une atteinte à l'intégrité de son territoire depuis 1939. Il en va à l'inverse avec la sécurité et par extension avec la cybersécurité. Et d'une certaine façon, le concept de cyberdéfense ne se justifie que parce qu'il revêt des enjeux régaliens. On l'a dit et vu, il est en effet de plus en plus malaisé de distinguer les attaques relevant de la cybercriminalité de celles s'apparentant à la cyberguerre (donc à la cyberdéfense si l'on suit la logique). Le continuum sécurité-défense, déjà dépassé car n'étant pas réellement d'ordre systémique, a toutefois le mérite de légitimer la notion de sécurité extérieure, beaucoup moins évidente que celle de sécurité intérieure, bien plus logique. La *cybersécurité offensive* regroupe en quelque sorte les deux approches : défendre le pays (et ses organisations) et ses SI mais adopter pour ce faire le point de vue des attaquants. C'est donc en tous points l'approche des hackers.

C'est en 1972 que James P. Anderson[818] inaugure et va démocratiser l'idée de tests d'intrusion comme moyen d'évaluer le niveau de sécurité des SI. S'il en fait partie, le *pentesting* n'est qu'une tactique parmi d'autres de la cybersécurité offensive. Celle-ci forme une stratégie mimétique consistant à penser comme des attaquants et ainsi imiter leurs tactiques, techniques, processus (TTPs) et outils en vue d'améliorer les mesures de protection. C'est pour cette raison que la sécurité défensive reste incontournable puisqu'elle se nourrit de l'approche offensive dans une logique permanente d'amélioration. Comme le fait remarquer très justement Victor Poucheret, « *L'asymétrie est dans le rapport attaquant/attaqué. Le défenseur, c'est tous les jours qu'il défend ; l'attaquant, s'il réussit, il gagne une fois et c'est terminé.*[819] » De ce point de vue, on le comprend, il est indispensable de renforcer au maximum sa sécurité. Mais cela ne peut passer que la compréhension et le jeu égal instauré avec les attaquants. Du moins en termes de savoir-faire technique et de connaissances des modalités d'attaques. Les hackers doivent donc être en formation permanente s'ils veulent se maintenir à niveau. Et c'est précisément ce qui les distingue car un hacker est avant tout un expérimentateur, « *quelqu'un qui regarde le monde avec curiosité, qui pose des questions, qui se demande toujours si autre chose est possible, ce que l'on pourrait faire, ce qu'il se passe si on prend une chose à part et qu'on la replace d'une façon nouvelle. Donc on peut dire que c'est un innovateur, un inventeur.*[820] »

[818] Eugene H. Spafford, « James P. Anderson: An Information Security Pioneer », *IEEE Security & Privacy Magazine*, 6(1), p. 9–9.
[819] Interview de Victor Poucheret et Brice Augras, chaine *Thinkerview*, *op. cit.*
[820] Keren Elazari, Conférence TED, *op. cit*.

Tant que les organisations disposaient leurs réseaux et systèmes en local, la cybersécurité défensive suffisait. Avec l'interconnexion des réseaux privés et le transfert d'actifs vers notamment des solutions de *cloud computing*, l'approche offensive est devenue impérative. Car les *hackers noirs* innovent tout autant sinon plus que les *chapeaux blancs*. Ainsi, les principales méthodes de sécurité offensive sont les suivantes :

- *L'évaluation initiale de la vulnérabilité*

Il s'agit de réaliser des tests et analyses de vulnérabilité à la fois manuellement (injections, tests de requêtes, scripts et logiciels spécialisés) et de manière automatisée (scanners) pour une plus grande efficacité. Les tests les plus superficiels se contenteront de l'approche automatique. Dans tous les cas, cela nécessite d'établir un rapport de failles exploitables selon une grille de criticité. La remédiation la plus basique consiste à appliquer des correctifs à ces failles ou à défaut de renforcer le système ou l'application vulnérable.

- *Les tests d'intrusion poussés*

Les pentesters réalisent ici des tests développés pour tenter d'identifier l'ensemble des failles d'un SI (systèmes, réseaux, applications web). Ces tests sont effectués selon trois modalités :

- en boite noire (*black box*) : aucune information n'est donnée sur la cible ;
- en boite grise (*grey box*) : certaines informations sont fournies au pentester ;
- en boite blanche (*white box*) : le pentester se voit communiquer le maximum de détails sur le SI, la topologie réseau et les utilisateurs (salariés…).

L'activité de *pentesting* nécessite une grande expérience et une formation constante, la plupart du temps mesurées et sanctionnées par des certifications spécifiques. La ou l'une des plus réputées, difficiles et complètes au monde est l'OSCP (*Offensive Security Certified Professional*), délivrée par Offensive Security (OffSec), une compagnie internationale d'origine américaine[821].

- *Le redteaming*

Une équipe rouge est formée de hackers éthiques à qui l'on assigne un objectif, une mission précise. Ça peut être le contrôle par élévation de privilèges d'un compte de niveau administrateur, accéder à une base de données particulière, etc. Le *redteaming* se distingue aussi par la mise en œuvre d'attaques physiques comme l'infiltration de locaux privés, par le biais de techniques d'ingénierie sociale. Face à cette équipe, une *blueteam* fait partie intégrante

[821] https://www.offsec.com/courses/pen-200/

de la cible et doit répondre aux attaques. Parfois, des équipes violettes (*purple team*) assurent la charnière entre la rouge et la bleue pour les coordonner et assurer un arbitrage.

- *Les simulations d'ingénierie sociale à distance (phishing)*

Les hackers élaborent des attaques « logico-humaines » via des simulations de *phishing* et ses variantes : *smishing* (par SMS), *vishing* (voie téléphonique) ou du ciblage personnalisé (*spear phishing/whaling*). Certaines sociétés de cybersécurité créent des jeux sérieux autour du phishing. Par exemple, Great-X est une entreprise toulousaine qui propose une *Room#42*, une salle immersive où l'on simule *in situ* des attaques de ce genre[822].

- *Veille cyber et de compromission / CTI*

Il s'agit d'assurer le suivi de son organisation sur le web (Pastebin, Github…) et le *Darkweb* (forums de revente de données/*dark markets*), de surveiller les fuites de données dont certains sites font par ailleurs légalement l'inventaire[823]. Cela permet d'anticiper leur exploitation à des fins d'attaques. À un niveau plus élevé, il sera question de renseignement sur la menace (CTI). Donc la CTI est une mesure de sécurité offensive avancée des plus efficace.

Au bilan, les hackers peuvent apporter leurs compétences spécifiques en matière d'approche offensive. Dans notre vision d'un état-major d'intelligence cyber, ils seraient donc en mesure d'assurer tout particulièrement ce volet. La proximité et la coordination avec le tissu économique des entreprises serait évidemment primordiale pour délivrer ce haut niveau d'expertise. Car un grand nombre d'entre elles prévoit au mieux mais n'anticipe jamais réellement les attaques cyber. En effet, il s'avère même que la plupart des managers sont insensibles à l'exposition aux agressions numériques. Du reste, ils n'appréhendent au mieux le risque qu'à travers la menace, donc en négligeant l'état de vulnérabilité interne de leur organisation ; s'en tiennent généralement à placer leur confiance dans les solutions uniquement techniques et une approche réactive[824]. Ce constat vient appuyer notre analyse sur la nécessité d'adopter un angle de sécurité offensive.

Dans ces deux volets (influence, sécurité offensive) et le troisième sur lequel nous conclurons, un dispositif intelligent requerra la mise en réseaux des acteurs nationaux. Les EUA eux-mêmes y souscrivent ou le rappellent : « *L'élaboration d'une stratégie nationale de cybersécurité, qui coordonne les agences et les ministères ainsi que les interactions avec les*

[822] https://www.capcobra.com/room42
[823] https://dehashed.com/ ou plus grand public : https://haveibeenpwned.com/
[824] C'est le bilan tiré des résultats d'une thèse de doctorat : Benoit Fantino, *Quels éléments d'influence pour l'adoption symbolique de la sécurité des systèmes d'information ?*, thèse de doctorat en sciences de gestion, université d'Aix-Marseille, 2018.

*entreprises privées et la société civile, est désormais le signe manifeste d'un État qui prend ses responsabilités.*[825] »

À cette fin et pour ce faire, notre dispositif va reposer sur la nécessité d'acquérir, intégrer et diffuser l'information en libérant la communication entre ces acteurs. Le renseignement, la fonction connaissance-anticipation est par conséquent une clé essentielle pour établir un dispositif intelligent.

### c) *L'OSINT comme pièce maîtresse du renseignement cyber*

L'intelligence cyber, au même titre que l'IE, va s'appuyer sur un pilier central qui précisément repose sur la définition française de l'anglicisme *intelligence*. L'information, ici numérique, est bien le matériau qui permet de générer des connaissances, les protéger et capitaliser dessus pour façonner l'environnement. Ce renseignement appliqué à l'espace numérique doit être décliné en quatre méthodes : le renseignement « sur », « par », « dans » et « pour » le cyber[826]. L'OSINT est un type de renseignement bien particulier : fondé sur les sources dites blanches (publiques) ou au pire grises (semi-privées), il repose sur une collecte passive et légale d'informations ne requérant aucun contact direct avec une cible et donc aucune technique de manipulation. Sa montée en puissance actuelle s'explique par l'explosion des sources ouvertes en particulier numériques. Ces dernières formeraient en effet près de 80% des informations accessibles[827]. Or, dans l'optique des nombreux appels lancés aux EUA par l'ex-officier Robert D. Steele, tout État se doit de disposer d'un service de renseignement de sources ouvertes. Au début des années 1990, et alors que la Commission Aspin-Brown évalue la communauté américaine du renseignement, Robert Steele met au défi les agences gouvernementales de produire des résultats plus pertinents que les siens. Convaincu qu'il peut obtenir des informations solides à partir de seules sources publiques, et armé d'un ordinateur et d'un téléphone comme seuls capteurs, il dresse en un jour une cartographie détaillée des secteurs politique, militaire, académique et économique sur le cas d'étude du Burundi. Bilan : la Commission pointe les lacunes du renseignement d'État concernant les sources ouvertes et recommande instamment d'y pourvoir[828]. En 2005 est alors créé l'*Open Source Center* (OSC), structure dédiée à la veille-analyse de l'information publique. Mais l'OSC reste sous la

[825] David Gioe, Tim Stevens, Michael S. Goodman, « Intelligence in Cyber Era: Evolution or Revolution? » *Political Science Quarterly*, 2020, pp. 191-224, p. 36.

[826] Yannick Pech, « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », *Prospective et stratégie*, 2019/1 (n°10), pp. 73-102.

[827] Les spécialistes s'entendent pour dire que l'information serait blanche à 80% (accès public, légal), 15% grise (accès légal mais non public) et 5% noire (accès illégal et privé, imposant une activité d'espionnage). Voir Franck Bulinge et Nicolas Moinet (dir.), « Le renseignement, un monde fermé dans une société ouverte », *op. cit.*, p. 19.

[828] Frédérick Douzet corrobore en disant que l'OSINT peut se révéler plus productif que le renseignement d'État (plus de moyens et de ressources démultipliés). Entretien avec l'autrice, 30/03/2022.

dépendance de la CIA, ce que stigmatise Robert Steele qui aspire à un service indépendant du gouvernement dans une logique d'intérêt commun. En avril 2006, il réitère[829]. Le *mouvement* de l'OSINT *numérique* est né et, s'il ne forme aujourd'hui qu'une petite sphère transnationale de passionnés, il n'en demeure pas moins dynamique, constituant une communauté visible sur des réseaux professionnels tel LinkedIn[830].

Le renseignement ouvert ne date donc pas d'hier mais il prend aujourd'hui un tour nouveau car il s'inscrit dans un phénomène de globalisation du renseignement. Au-delà d'une privatisation entamée à la fin du XX^e^ siècle, renseignements public et privé s'imbriquent aujourd'hui toujours davantage. En effet, si l'intelligence économique est fille du renseignement, à son tour a-t-elle influencé considérablement ce dernier. La veille informationnelle s'est inspirée largement du *cycle du renseignement*, et les entreprises sensibilisées à ces problématiques ont très tôt fait appel à d'anciens officiers reconvertis dans le privé, pour le meilleur mais aussi parfois le pire[831]. Ce mariage d'opportunité semble toutefois avoir trouvé ses lettres de noblesse aujourd'hui. En particulier, les considérations déontologiques de l'IE ont infusé dans le monde du renseignement, comme en atteste la réflexion éthique portée à ce sujet tant par les universitaires que par les professionnels de la profession. Ainsi, une dynamique de percolation privé-public s'est opérée qui a démocratisé le renseignement auparavant monopole d'État.

On l'a évoqué à plusieurs reprises, la *cyber threat intelligence* s'inscrit parfaitement comme charnière entre renseignement ouvert et fermé. Ainsi, la CTI s'avère intéressante car elle s'appuie, tout en le renouvelant, sur le cycle du renseignement pour orienter son action[832]. Si elle n'en oublie pas les aspects – nécessairement – techniques[833], elle concentre en réalité son approche sur l'analyse humaine, notamment parce qu'elle requiert des techniques d'OSINT. De plus, elle semble assurer le lien entre cybersécurité et cyberdéfense, tactique et

[829] Voir Annexe 3 ; Robert D. Steele, *On Intelligence: Spies and Secrecy in an Open World*, OSS International Press, 2001, 496 p.

[830] Notamment certains groupes privés ouverts à la cooptation. Bellingcat.com, créé par un ancien journaliste d'investigation britannique, reste une référence. En France, se distingue le blog rattaché au journal *Le Monde*, Bug Brother, ou encore le site securiteoff.com. On a déjà parlé d'openfacto.fr, osintfr.com ou ozint.eu. D'autres spécialistes, comme l'Américain Michael Bazzell ou un ancien officier du renseignement néerlandais, proposent des formations à ces techniques d'investigation (https://inteltechniques.com).

[831] Franck Bulinge, *De l'espionnage au renseignement*, *op. cit.*, pp. 251-252.

[832] Un rapport de 2013, actualisé en 2019, évoque le dépoussiérage dudit cycle. https://resources.sei.cmu.edu/asset_files/EducationalMaterial/2019_011_001_546699.pdf. Ses auteurs proposaient d'amender le modèle pour l'appliquer à la dimension cyber. Ainsi, entre collecte et diffusion, la phase de traitement couplerait une « analyse technique » de la menace destinée à définir le « quoi » et le « comment » des cyberattaques ; et une « analyse stratégique » visant une contextualisation holistique des incidents cyber pour répondre à la question du « qui » et du « pourquoi ». En 2011 apparaissait l'expression CTI.

[833] Sur la base du concept d'informatique forensique d'*indicateurs de compromission* (IoC).

stratégie, public et privé – les entreprises mettant parfois en place une véritable « défense » plutôt qu'une simple sécurité (homologations, certifications, normes).

En définitive, l'essor de l'OSINT fait écho aux célèbres vers de Racine dans *Britannicus* : « *Il n'est point de secret que le temps ne révèle* ». À l'âge de l'hypertransparence et de l'infocommunication en temps réel, ils se révèlent d'une prégnante acuité. Ainsi, tout acteur peut produire du renseignement, y compris l'individu, véritable « *caporal stratégique* » en puissance. Le complexe public/privé voit donc remise en cause sa dichotomie traditionnelle. Désormais, la plupart des acteurs privés ont investi le champ numérique qui, pour certains d'entre eux, s'avère exclusif et donc indispensable à leur visibilité. En particulier, les ONG militantes ou les mouvements sociaux exploitent très efficacement l'indiscutable caisse de résonance que constitue le cyberespace. Le cas de la « sous-veillance » éclaire d'un jour nouveau les applications d'un « renseignement ordinaire »[834]. En 2018, la crise des *Gilets jaunes* a montré la pleine dimension de cette « panoptique inversée » où le surveillé se fait surveillant. Confrontés désormais aux capacités de captation et de couverture en temps réel d'un évènement, les États – démocratiques ou non – ont bien du mal à canaliser l'activisme de ces « journalistes-citoyens ». Ici, la pervasivité de la sphère numérique permet à de simples possesseurs de smartphones d'*info-communiquer* à travers des applications comme Telegram, Facebook Live ou encore Twitter/X. De la même façon, l'association animaliste et antispéciste L214 montre, au-delà même de la question des moyens d'acquisition de ces images privées, comment un acteur « lambda » (deux individus fondateurs) peut exercer une influence dans notre espace communicationnel. Ses vidéos postées sur le média social YouTube ont fait ainsi le tour de la planète[835].

À cette problématique vient par ailleurs se greffer l'enjeu de ce qu'on appelle communément les « *leaks* » ou fuites d'informations privées, ainsi que la question des lanceurs d'alerte. Prenons l'exemple déjà évoquée de l'affaire « Disclose »[836], ayant trait à une note de renseignement (DRM). Pour rappel, celle-ci ferait état de l'utilisation par l'Arabie saoudite de systèmes d'armes français dans la guerre qu'elle mène au Yémen depuis 2014. Quelle que soit l'exactitude de ces accusations et les conséquences induites, c'est l'impact de cette communication qui compte davantage : en effet, la France est partie au Traité international sur le commerce des armes (2014), engageant ses signataires à ne pas en vendre à un État en

[834] Camille Alloing, « La sousveillance. Vers un renseignement ordinaire », *Hermès*, *op. cit.*, pp. 68-73. Par-delà la sousveillance, la « sous-surveillance » vient mutualiser les connaissances des militants sur les structures et dispositifs technico-juridiques déployés par les autorités publiques. Voir par exemple https://www.sous-surveillance.net ou https://www.lemonde.fr/blog/bugbrother. On peut aussi mentionner le travail des cartographes amateurs, dont l'un des représentants les plus connus est le projet Liveuamap, né pendant la guerre syrienne (https://liveuamap.com).

[835] https://www.l214.com/

[836] https://made-in-france.disclose.ngo/fr/chapter/yemen-papers.

guerre. Or, si l'ONG s'est basée sur le lancement d'alerte exclusif d'un ancien cadre du MINARM[837], ses équipes de journalistes, juristes ou encore chercheurs et RSSI ont réalisé des recoupements à partir de sources ouvertes. On en revient à la problématique d'un monde fermé (le renseignement et le secret d'État) dans une société ouverte, mettant en exergue le dilemme classique des démocraties, entre préservation du secret-défense et logique de transparence.

Plus prosaïquement, l'OSINT se fonde aussi sur les négligences en tous genres et les externalités négatives des numérisation et généralisation des données ouvertes. On a déjà évoqué la méthode du *Google Dorking*, qui requiert un certain entrainement avant de devenir une simple gymnastique. Mais d'autres techniques d'OSINT ne nécessitent aucune compétence particulière. C'est le cas avec des outils cartographiques grand public tels que Google Maps. Utilisés à des fins plus ou moins respectables, ils peuvent se révéler d'une redoutable efficacité. L'exemple de l'évasion d'un détenu français a défrayé la chronique en juillet 2018. Le 1er du mois, Redoine Faïd s'évade au moyen de l'hélicoptère qui vient de se poser au milieu de la cour du Centre pénitentiaire de Réau. Le 31 juillet, le ministère de la Justice transmet un courrier à Google pour que soient floutées les images aériennes des prisons françaises. Les malfaiteurs s'étaient-ils servis de ces informations publiques ? Toujours est-il que le recoupement d'éléments de « ROHUM-R » et de GEOINT pouvait être réalisé pour faciliter le repérage des dispositifs de sécurité physique de l'établissement[838].

Autre exemple, la nature et le volume croissant des contenus échangés sur les réseaux socionumériques ont motivé l'idée d'établir une sous-discipline du ROSO, baptisée ROMESO ou *renseignement d'origine média sociaux*[839]. Les fonctionnalités de recherche interne de ces plateformes constituent autant d'outils capables de capter des informations sur diverses thématiques : tendances sociétales ou de consommation, vie privée[840], prémices de mouvements sociaux en devenir, stratégies de communication, influence, campagnes de

[837] https://www.lemonde.fr/actualite-medias/article/2023/09/21/remise-en-liberte-de-la-journaliste-du-site-disclose-a-l-origine-du-scandale-sirli_6190240_3236.html

[838] Plusieurs mois après la requête déposée par l'État français, plusieurs prisons étaient toujours visibles. Les impératifs et agendas d'entreprises comme Alphabet ne sont évidemment pas ceux des gouvernements ; sans parler des tensions entre certains États européens et la société californienne.

[839] En anglais : SOCMINT, *Social Media Intelligence*. Des outils de veille-analyse de ces réseaux sont commercialisés ou certains sont gratuits (ex. : https://onemilliontweetmap.com).

[840] Le cas emblématique du « Graph Search » (et sa fonction *StalkScan*) de Facebook avait défrayé la chronique lors de son implémentation en 2013. En effet, il permettait d'interroger par phrases-clés l'intégralité des données personnelles renseignées par les utilisateurs sur leur compte. Partiellement désactivé (accès « gris ») sur la plateforme, il a finalement été mis en pause en juin 2019. Ce dont se sont émus spécialistes OSINT et journalistes.

« réinformation »… Autant de sujets intéressant les entreprises bien sûr[841], mais aussi les États (dont le fisc) ou les ONG militantes[842].

Enfin, tout aussi significatifs et de plus en plus médiatisés : les cas de divulgations de données personnelles liées aux usages non maîtrisés – plutôt que non maîtrisables – des technologies de l'information. Citons l'application dédiée aux sportifs Strava ou celle consacrée à la cartographie, Polar, dont les fuites se sont révélées particulièrement préjudiciables à plusieurs armées et services de renseignement nationaux[843]. Fruits de la combinaison de sites ou applications non sécurisés et de leurs mésusages, ces affaires ont du moins le mérite de montrer qu'en faisant de l'OSINT, on peut aussi opportunément détecter des vulnérabilités : failles techniques ou négligence des éditeurs de logiciels, failles humaines des utilisateurs. Le principe de « sécurité par la transparence »[844] n'est pas loin. Finalement, la question que pose la démocratisation de ces techniques est celle de la criticité des informations qu'il est possible d'en tirer dans un contexte de transparence accrue. Comme en atteste le combat mené par des lanceurs d'alerte – à leur façon – comme Robert Steele, l'argument final de l'OSINT (technique) et du renseignement privé (pratique) est la production de connaissance-intelligence. Et si « *les espions sont parmi nous* »[845], reste que faire du renseignement, même ouvert, n'est pas à la portée de tous. Des spécialistes tirent leur épingle d'un jeu requérant connaissances techniques et « humaines ».

Les hackers peuvent dès lors nous aider. Collecte d'information, scan de vulnérabilités web, rétro-ingénierie, cryptanalyse[846], kits d'ingénierie sociale, « écoute réseau », création d'*exploits*, investigation forensique… En réalité, le hacking est :

> « *clairement du renseignement. Le hacking est une pénétration dans la bulle du secret, grâce à l'agrégation d'informations*. […] *L'OSINT est un sas d'entrée incontournable pour connaître les développeurs, webmasters, informaticiens et leur manière de penser, leur background, leurs patterns, les technologies utilisées (matérielles, logicielles-applicatives), leurs passifs (comptes leakés, documentation exploitable…), le floutage entre les activités de vie privée et publique, professionnelles et personnelles. L'OSINT*

[841] En outre, certaines d'entre elles, comme Airbus, financent des thèses CIFRE portant sur les recherches appliquées au SOCMINT.
[842] Du reste, d'aucuns parlent « d'arsenalisation » des réseaux. Peter W. Singer et Emerson T. Brooking, *LikeWar: The Weaponization of the Social Media*, Houghton Mifflin Harcourt, 2018, 421 p.
[843] https://www.lemonde.fr/pixels/article/2018/01/29/la-securite-des-bases-militaires-menacee-par-une-application-de-jogging_5248885_4408996.html;https://www.lemonde.fr/pixels/article/2018/07/09/des-centaines-d-espions-et-de-militaires-identifiables-a-cause-d-une-application-sportive_5328595_4408996.html.
[844] Possibilité d'auditer le code informatique des logiciels, dès lors que celui-ci est ouvert (*open source*). Son pendant fermé est appelé « sécurité par l'obscurité » : le code source est alors dit « privateur » ou propriétaire.
[845] Nicolas Moinet, *Les sentiers de la guerre économique. L'école des nouveaux* espions (vol. I), VA, 2018, 192 p.
[846] La cryptanalyse consiste à décrypter ce qui est chiffré. On ne dispose pas de la clé de chiffrement qui permettrait de déchiffrer, donc on utilise des techniques (attaques par force brute, attaques par dictionnaires…) pour décrypter. Il est par conséquent erroné d'indifférencier les termes français *décrypter* (« crypter » n'étant pas français) et *déchiffrer* : si on vole la clé ouvrant telle serrure, on n'a pas besoin de fracturer cette dernière.

> *c'est du hacking car il y a la même philosophie de la "bidouille", donc un OSINTer est un hacker. Il y a le même état d'esprit de se dépasser ; de se remettre en question sur la perception d'une image, d'un phénomène ; et de remettre en question le fonctionnement d'une chose, d'une machine.* […] *C'est de la "bidouille intellectuelle". Pas au sens spécifiquement technique, bien qu'il y ait des OSINTers doués en informatique. Ce n'est pas une discipline spécifique. Les hackers font d'ailleurs de l'OSINT, et le cycle du hacking comporte cette collecte dite passive d'informations.*[847] »

Les hackers font donc ni plus ni moins du renseignement : ils exploitent l'information blanche ou grise pour se frayer un chemin vers l'information noire, au même titre que les SR. Au bilan, notre état-major d'intelligence cyber saisirait cette opportunité pour ainsi créer un service d'OSINT qui échangerait notamment avec des *sociétés d'économie numérique* – productrices de veille –, elles-mêmes en interaction avec les entreprises privées nationales. Ainsi, en combinant harmonieusement la triade OSINT–cybersécurité offensive–influence, les hackers trouveraient toute leur place au sein de ce dispositif intelligent.

Il convient à ce stade final de dresser un bilan scientifique de notre travail de recherche. Ce faisant, seront tirés les enseignements de cette thèse de doctorat, évoquées ses limites et esquissée une réflexion sur des pistes de développement.

[847] Entretien avec Victor Poucheret, 14/11/2021. Florent Curtet, Julien Métayer, Clément Domingo, ainsi qu'Alexandre Oda dans une large mesure souscrivent et mettent en avant la « reconnaissance passive » que constitue l'OSINT, mais que les hackers doublent d'une « reconnaissance active », à savoir la partie offensive basée sur l'interaction avec les cibles à travers l'ingénierie sociale.

# CONCLUSION :
# LIMITES ET PERSPECTIVES DE RECHERCHE

## 1) La démarche abductive : limites et pertinence

En premier lieu, au regard du choix opéré pour notre étude, les cas sélectionnés posent la question des conditions d'accès à ce genre d'informations plus ou moins ouvertes. Si nous n'avons même pas ambitionné de contacter par exemple la DGSE – et pour l'avoir déjà fait dans le cadre d'un autre travail de recherche[848] –, c'est que nous ne connaissons que trop bien le culte du secret dont le service s'entoure. Du reste, nos demandes d'entrevues infructueuses auprès d'anciens membres de la « piscine[849] » en attestent, alors qu'ils ne sont par définition plus actifs. Si un officier de la DGSI a bien voulu s'entretenir avec nous, cela n'a pas amené à des résultats très probants. Les choix de nos cas étaient donc très contraints, et nous avons d'ailleurs été bien en peine de les identifier en premier examen. Néanmoins, en regardant l'autre versant de la montagne, approcher le sujet à travers des cas qui ont souvent révélé leur intérêt *a posteriori* nous amène à penser que certains biais ont pu être évités, et notamment celui de confirmation, possiblement l'effet de halo ou celui de cadrage. La démarche abductive permet en principe de ne pas se raccrocher à des certitudes ou une théorie générale par trop catégorique, écueil qui peut guetter l'inférence déductive[850].

En second point, il faut admettre, comme nous l'avons mentionné dès l'introduction générale, que la démarche abductive est assimilée à une approche relative voire relativiste de la scientificité. Elle est de ce fait très associée aux approches constructivistes. L'épistémologie du pragmatisme/constructivisme établit en effet que la science est un état donné de connaissances, un état de croyances en réalité provisoires voire transitoires. Dans cette optique, les faits sont situés historiquement et culturellement, d'où des données empiriques problématiques et partielles. Thomas Kuhn, grand penseur du concept de paradigme, ne dit pourtant pas autre chose, mettant en exergue la dimension nécessairement provisoire des visions du monde qui amène la science à définir ce que l'on sait à un moment donné, mais qui peut s'effondrer sous le poids d'une vision qui remplacera la précédente et sera à son tour *a priori* incontestable[851]. Ce cycle de la science est au vrai normal et fondé sur la dialectique du

[848] Yannick Pech, *L'influence du renseignement…*, *op. cit*.
[849] Surnom donné au siège de la DGSE, voisin de la piscine des Tourelles et sis boulevard Mortier à Paris.
[850] Nous connaissons bien cela, puisqu'en science politique-Relations internationales, le chercheur doit quasi-impérativement s'inscrire dans un courant théorique par défaut, laissant peu de liberté d'innovation ou alors marginale (par entregreffage théorique) et obligeant de vérifier une hypothèse préétablie.
[851] Thomas Kuhn, *La Structure des révolutions scientifiques*, Flammarion, 1992 (rééd. 2008), 352 p.

doute et de la croyance. Le premier requestionne en permanence la seconde qui reste « *un moment d'arrêt dans notre activité intellectuelle, un effet produit sur notre être par la pensée et qui influe sur la pensée future*.[852] » Ceci étant dit, et sans développer ici davantage, l'abduction semble en tout état de cause s'adapter tout particulièrement à notre travail.

* * *

« *Nous savons que nous ne savons pas. C'est ce doute-là qui est le moteur de la recherche*.[853] » nous dit le physicien et philosophe des sciences Étienne Klein. Depuis Aristote dans son *Organon*, en effet, l'abduction a été pensée comme une démarche d'inférence logique propre à comprendre plutôt qu'à expliquer les phénomènes. Elle permet d'ailleurs de préparer un travail empirique et de réduire le champ à étudier. Surtout, elle exploite les deux autres inférences conventionnelles dans un cycle récursif à même de questionner ce que l'on sait ou croit savoir. La démarche abductive se fonde sur un étonnement face à un fait (surprenant ou anormal) sans explication et cherche à faire émerger des idées nouvelles[854]. Ainsi, elle est *ampliative* : elle augmente la connaissance et, se plaçant entre la déduction qui « *prouve que quelque chose doit être ; l'induction qui montre que quelque chose est réellement agissant* », elle « *suggère que quelque chose peut être*.[855] » L'on peut dès lors considérer que l'approche qualitative de notre travail de recherche est venue questionner un fait anormal ou surprenant : pourquoi ne pas intégrer dans le dispositif national de cybersécurité ceux qui comptent parmi les meilleurs spécialistes de l'informatique et des technologies numériques, à savoir les hackers ?

En somme, la démarche abductive est un exercice « d'instinct rationnel » s'appuyant sur un fil conducteur : le doute, et favorisant la création d'hypothèses parmi plusieurs possibles tout en sous-tendant une logique argumentative. Si elle peut flirter avec le principe du rasoir d'Ockham (nous avons opté pour trois hypothèses dont une médiane), elle doit être pour autant soumise à l'épreuve de la réalité empirique.

[852] Charles S. Peirce, cité par Yves Hallée & Julie M. É. Garneau, « L'abduction comme mode d'inférence et méthode de recherche : de l'origine à aujourd'hui », *op. cit.*, p. 127.
[853] Prononcé lors une émission radio sur France inter (https://www.youtube.com/watch?v=RwnicOFHehc).
[854] Javier Nuñez Moscoso, « Et si l'on osait une épistémologie de la découverte ? La démarche abductive au service de l'analyse du travail enseignant », *op. cit.*, p. 7.
[855] Javier Nuñez Moscoso, *ibid.*, p. 10.

Voici schématisée la boucle récursive dite « ADI » :

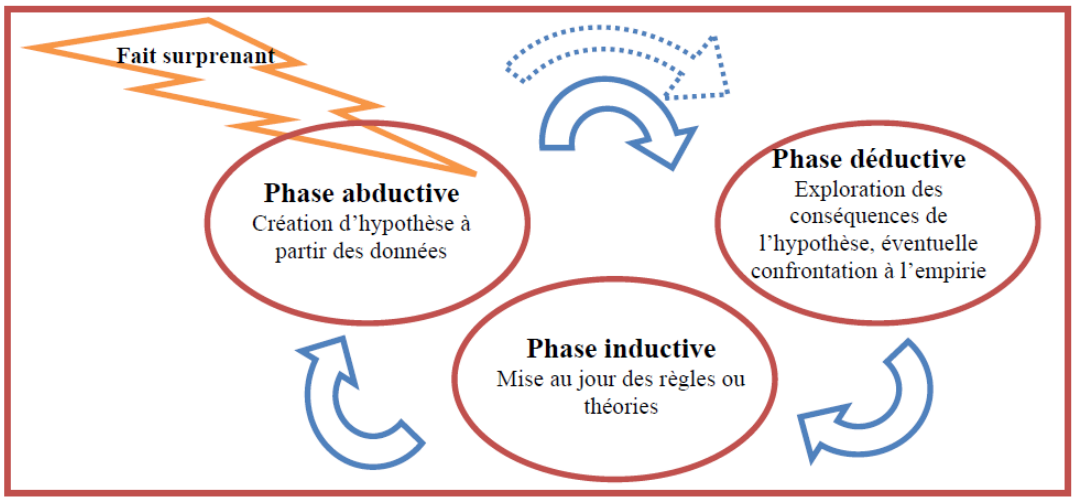



**Figure 48 :** *Boucle récursive des trois phases : Abduction-Déduction-Induction*

Source : Javier Nuñez Moscoso, *op. cit.*, p. 12.

Ainsi, à partir de nos observations préalables dans le milieu de la cybersécurité et des premières données collectées à travers les entretiens, nous avons pu tirer une batterie d'hypothèses exploratoires fondées sur une orientation théorique flexible et néanmoins cadrée afin de ne pas être noyé par les données ultérieures (A). Puis, nos hypothèses nous mènent à développer un volet théorique à même de guider notre analyse à l'aune des sciences de l'information et de la communication, dont l'IE peut articuler les deux axes pour les croiser avec la stratégie et la notion de dispositif intelligent. Nous formalisons dès lors notre démarche initialement « instinctive » en la rationnalisant (D). Enfin, nous évaluons les résultats du contraste entre les hypothèses et le test empirique, notamment en naviguant entre entretiens et volet théorique pour la mise au jour d'une grille de lecture. Notre « immersion » via une meilleure compréhension du hacking (formation en *pentesting*, participation à des CTF, contacts et discussions avec des hackers) nous aidant à affiner notre perception des phénomènes. L'on recherche alors à analyser des cas aux caractéristiques similaires. Au fil des cas étudiés, l'hypothèse médiane est validée, donc on ne relance pas la boucle et on maintient notre grille théorique (I).

En définitive, la démarche abductive consiste à poser un regard critique pour approcher une connaissance plausible ou probable. De surcroît, en cherchant à comprendre les phénomènes, elle peut tenter de les « transformer » via un volet heuristique (« croyance ») et une approche praxéologique, voire prescriptrice. Ceci nous ayant amené à la formulation de préconisations, qui ont fait l'objet du chapitre 6.

Il nous faut énoncer une autre limite à notre travail. D'abord, sur quel référentiel envisager ce qui relève d'une situation de communication, d'incommunication ou d'acommunication ? Autrement dit, est-ce que notre évaluation du degré de communication peut être rationnalisée ? Si l'acommunication semble plus facile à jauger, la différence entre une situation de communication et d'incommunication n'est pas toujours évidente. De même, si incommunication il y a, cette situation ne revient-elle pas en définitive à parler d'acommunication (pas de volonté réelle de synergie, collaboration contrainte mais peu souhaitée, relation biaisée et asymétrique…) ? [856]

Par ailleurs, si les relations entre hackers et autorités politico-sécuritaires ont été volontiers traitées dans le cadre de notre travail, nous avons finalement accordé moins de place aux rapports entre les hackers et les entreprises privées. Les hôpitaux ont pu être présentés comme des équivalents possibles, étant donné par ailleurs leurs conditions difficiles et contraintes par des impératifs budgétaires, mais ils n'en demeurent pas moins des services publics. Toutefois, les organisations privées ont été à plusieurs reprises évoquées, surtout à travers le croisement des témoignages de nos interviewés.

Après ces éclaircissements et interrogations sur la démarche adoptée, il convient d'esquisser une ouverture de ce travail de recherche.

### **2)** Perspectives : intelligence économique et cyber, un croisement fécond

**En appliquant l'intelligence économique aux enjeux de l'espace numérique, nous transposons en définitive la maxime de celle-ci dans un champ augmenté de la réalité conflictuelle : si l'IE est le croisement de l'information et de la stratégie, l'*intelligence cyber* est celui de l'information numérique sur un plan aussi bien technique que sémantique avec une stratégie de milieu**. Un milieu, on l'a dit, transverse. Partie de l'IE, l'*intelligence cyber* projette toujours plus la réalité en données dans un espace greffant monde matériel et sphère immatérielle articulés par le code. Si l'on a établi le postulat d'une guerre économique/systémique et fait le constat à tout le moins d'une cyberguérilla, dès lors il est loisible de penser qu'au même titre que l'IE requiert une approche pragmatique de la conflictualité, le cyber doit être pensé comme un facteur de puissance et un vecteur d'influence. Ainsi doit être assumée la cyberconflictualité à une échelle globale et non strictement militaire, embrassant les trois champs de la rivalité systémique : affrontement,

[856] Pour mieux définir cette nature et ce degré de communication, un développement intéressant pourrait être envisagé en appliquant le modèle de communication systémique d'Alex Mucchielli. Voir Alex Mucchielli, « Pour des recherches en communication », in "La recherche en communication", *Communication & organisation*, ISIC-GRECO/O, n°10, 1996.

contestation et même compétition. Dans cette optique, reprenons le tableau comparatif des courants paradigmatiques de l'IE pour le transposer au cyber :

| **Cyberguerre/ infoguerre** | **Sécurité numérique** | **Compétitivité de l'économie numérique** | **Diplomatie (du) numérique** |
|---|---|---|---|
| International/ transnational | International/ intranational | Public-privé | International/ transnational |
| Volonté de cyberpuissance | Intérêts nationaux et souveraineté numérique | Libéralisme et mondialisation maîtrisée | Stabilité du cyberespace |
| La guerre par d'autres moyens (*contestation*) | La cybersécurité comme approche | La compétitivité comme règle | Responsabilité et rationalisation |
| Conflictualité assumée | Conflictualité subie/résilience | Conflictualité non assumée | Conflictualité négociée |
| Culture du renseignement et du hacking (opé. spéciales) | La *threat intelligence* comme contre-mesure | Prisme du mercenariat économique | Transition éconumérique/ maîtrise des armes numériques |

**Figure 49 :** *Essai de transposition des courants de l'IE à l'intelligence cyber*

Source : basé sur Franck Bulinge & Nicolas Moinet, « L'intelligence économique : un concept, quatre courants », *op. cit.*, p. 62.

Au bilan, si les points de vue divergent sur l'approche que doit adopter l'IE et par extension l'*intelligence cyber*, les faits sont têtus et illustrent sempiternellement les réalités d'un monde fondé sur une conflictualité intersubjective, liée vraisemblablement à une part irrépressible des nature et culture humaines. Vouloir déjouer et d'abord savoir identifier les attaques informationnelles et informatiques de nos ennemis, adversaires et pseudo-alliés, c'est accepter les mots d'apparence paternaliste et dédaigneuse mais une réalité somme toute pragmatique exprimée par Hubert Védrine : « *Les Européens modernes* [sont] *des gentils Bisounours perdus dans Jurassic Park*.[857] »

Pour les tenants du postulat de la guerre économique, il semblerait donc que nos élites politiques soient encore placées dans une logique de compétitivité libérale où, d'une part, le marché du numérique appartient aux plus innovants, entre États-Unis et Chine en particulier ; d'autre part, que l'économie numérique s'autorégule naturellement. Étant entendu que l'Europe n'a jamais souhaité ni même seulement envisagé d'être partie prenante à cette

[857] Hubert Védrine, *Et après ?*, Fayard, 2020, 144 p., p. 82.

concurrence, jusqu'à tuer dans l'œuf de possibles leaders continentaux par ses politiques antimonopolistiques hors-sol (pensons à Siemens et Alstom) et à rebours des pratiques internationales. Notons certaines avancées encourageantes comme le projet – tardif – d'ouverture d'une filière de production européenne de semi-conducteurs. Si la France a frayé la voie d'une approche offensive en termes de cyberdéfense, en lien avec un volet de sécurité numérique, se positionner constamment entre deux eaux dénote et favorise à la fois un manque de clarté stratégique. Comme l'explique la chercheuse allemande Lisa Cohen, de l'Institut de droit du maintien de la paix de l'université de la Ruhr, les États rechignent à parler de cyberguerre vraisemblablement parce qu'ils ne savent pas se positionner par rapport à cette complexité, et que ça induirait des problèmes inextricables dans leurs relations et le droit international[858]. Du moins est-ce la position lénifiante de la diplomatie des États européens.

La France peut-elle alors assumer la cyberconflictualité, sur l'échiquier de la contestation comme celui de la compétition globale, en vue de « *gagner la guerre avant la guerre* » ? Prétendre au statut de cyberpuissance induit, en effet, de se donner les moyens de ses ambitions et de se fixer un cap stratégique.

* * *

Arrivé au terme de ce travail de recherche, vient le temps d'en clore la réflexion bien entendu toujours en mouvement. Si, pour reprendre les mots du poète Zong Ze, la (cyber)stratégie n'a pas sauté directement aux yeux des institutions publiques et privées c'est, nous le pensons, pour plusieurs raisons.

*Primo*, la stratégie appliquée au cyberespace ne peut faire l'économie d'un élargissement du champ de vision des acteurs et ne doit se cantonner à l'aspect strictement militaire du domaine à travers une cyberdéfense. Au même titre que prévoir n'est pas anticiper, que la sécurité n'est pas qu'une simple protection, la cybersécurité doit embrasser l'ensemble du spectre des activités civiles et militaires pour en unifier la stratégie, défensive et offensive, à un niveau global. Cela nécessite une vision politique porteuse à même de redonner du sens au roman national dans un contexte mondial qui, s'il y avait besoin de le repréciser, montre ses tensions et ses lignes de partage profondes et intrinsèques dans la compétition globale. Un sursaut est nécessaire pour retisser du lien et resolidariser les forces vives du pays. Car la cybersécurité est avant tout une affaire humaine avant d'être un imbroglio technologique.

*Secundo*, élaborer une stratégie requiert d'utiliser des moyens en vue d'une fin. Or, pour ce faire, il est impératif de trouver des moyens. Notre travail a permis de constater à cet égard

[858] Carolin Riethmüller, *in Cybercriminalité, des attaques bien réelles*, Arte, *op. cit.*

que les services publics et une bonne part des entreprises en assignent justement peu dans la sécurité informatique. Les budgets qui y consacrés sont en effet très faibles, sans compter les ressources d'ordres organisationnel et humain qui font figure de parents pauvres. L'équation n'est certes pas simple, notamment pour les établissements hospitaliers où les priorités sont bien logiquement ailleurs. La situation est moins acceptable en revanche pour les entreprises privées, lesquelles ne nécessitent pas de mettre en place des solutions coûteuses là où, encore une fois, l'aspect organisationnel et la sensibilisation des personnels sont la clé pour une meilleure protection.

*Tertio*, les moyens à allouer à la cybersécurité ne sont ni ne doivent relever que d'aspects financiers et techniques contrairement à la croyance ancrée chez la plupart des acteurs. En effet, la sécurité numérique ne peut se résumer à la mise en place de mesures ou de solutions technologiques « clé en main ». C'est avant tout une culture, qui doit être diffusée et intégrée à tous les échelons, dans la perspective d'émergence d'une *intelligence situationnelle distribuée* où tous les acteurs d'une chaine forment les maillons forts. Au centre de ce dispositif, les hackers peuvent représenter les meilleurs candidats à la structuration d'un système où l'on conçoit la sécurité *by design*. Si intrinsèquement les technologies numériques permettent de libérer le potentiel de communication et de synergie entre acteurs, et de générer naturellement le réseau et favoriser l'intelligence collective, elles ne doivent pas devenir l'objet d'une gadgetisation ou d'un fétichisme et faire oublier la sécurité. En somme, il convient de **cloisonner la donnée, déverrouiller l'information.**

Or, les enseignements tirés de notre travail de recherche nous amènent à penser que les hackers ne sont pas considérés à leur juste valeur et que les liens friables qui les relient aux institutions publiques et privées n'autorisent pas la mise en place d'un dispositif intelligent à même de structurer un cadre solide de cybersécurité nationale. Si comme le dépeint Victor Poucheret, « *l'écosystème informatique est de l'ordre de la planète et de l'impact de la perte de la biodiversité.*[859] », il est temps de faire davantage confiance à ses coreligionnaires pour limiter le tarissement de l'environnement numérique. D'esprit naturellement offensif, les hackers font écho à la parole du célèbre bretteur japonais, Miyamoto Musashi, pour qui en tactique comme en stratégie, il s'agit de devancer l'adversaire. En d'autres termes, même si l'on n'a pas l'initiative de l'attaque, il faut anticiper son mouvement et saisir l'initiative de la contre-offensive. « *Prendre l'initiative signifie parvenir à la victoire sous l'effet de l'intelligence* ». Les hackers étant les mieux placés pour comprendre les attaquants, « *Devenez votre adversaire.*[860] »

[859] Interview de Victor Poucheret, chaine *Thinkerview*, 24/09/2021.
[860] Miyamoto Musashi, *Traité des Cinq Roues*, chapitre du Feu, Albin Michel, 1983, 188 p., pp. 100-103, p. 109.

Pour conclure, laissons la parole à Marc Sejean, qui dresse ce constat volontariste :

> **« *Il faut une réelle volonté politique, une synergie.* [...] *On est plein d'acteurs différents et en cybersécurité, il faut accorder nos violons.* [...] *On sait comment certains pays fonctionnent* [...] *En France, il est toujours complexe de passer réellement à l'attaque. C'est très compliqué, on est une démocratie, un État de droit, et on doit se battre contre des pays qui ont des structures moins monolithiques où il y a une perméabilité entre les services secrets, les mafias et les cybercriminels.* [...] *Et nous, en France, encore une fois, on ne pourrait pas fonctionner comme ça, mais je pense qu'il y a vraiment tout à inventer.* [...] *Il y a vraiment une synergie qu'il faut apporter entre les différents acteurs.*[861] »**

[861] Marc Sejean, Conférence CyberNeTic du 27/04/23, IUT Bordeaux-Montaigne.

# ANNEXES

# **ANNEXE 1 :** Flash sur la situation cyber dans nos hôpitaux

https://www.linkedin.com/pulse/enqu%25C3%25AAte-flash-sur-la-situation-cyber-dans-nos-h%25C3%25B4pitaux-florent-curtet?trackingId=Ce2wJHMzSdSnrBf52ky41A%3D%3D&lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_content_view%3BP%2BtoRjNFQymSDg5SZczIWA%3D%3D

**Florent Curtet**
Ecrivain @ Hacke-moi si tu peux // Co-Fondateur @ HSF // Dir @ NEO Cyber
5 articles
21 septembre 2022

**Quel été…**

Dans l'art et les règles de la guerre, confirmé par le droit international et humanitaire, les acteurs de santé sont affiliés par une neutralité et estampillés apolitiques. Nuls ne sauraient les mettre en joue, les capturer, ou encore de les empêcher d'exercer leur métier profondément humain.

Cependant, dans le cyber, il semble que certaines crapules fassent fi de ces règles humaines inaliénables, qui sont empiriquement respectées depuis déjà plusieurs siècles.

**Après le piratage de l'Hôpital de Corbeil, Hackers Without Borders a pris la décision de faire un audit dans trois différents hôpitaux français, afin d'avoir une visibilité globale de la cyber-santé des établissements médicaux :** ceux-là même qui, quelque soit notre soucis de santé, et à toute heure, seront toujours présent pour nous soigner. Ils ont aidé nos mères à nous donner la vie, et accompagnent nos anciens jusqu'au dernier souffle.

C'est dans cette optique, avec un mélange d'émotion et d'incompréhension que nous avons grossièrement fait un bilan-santé cyber du patient "Hôpitaux de Paris". Afin de pouvoir se rendre compte de la vulnérabilité de nos structures de santé si précieuses.

Pour cette analyse, trois hôpitaux ont été mis au bloc opératoire. Parfois avec une méthode white box, et d'autres un peu plus précises, en interviewant directement le corps médical de ces derniers.

Voici les points que nous avons pu relever :

Pour un service lambda de chirurgie (je ne nommerai pas les spécialités, mais c'est finalement une généralité.):

Concernant la segmentation des habilitations, il existe, dans l'écrasante majorité des cas cinq types de profils utilisateur :

- Intérimaires,
- Stagiaires,
- Vacataires infirmiers, aides-soignants,
- Contractuels : le médical (internes et externes) et le paramédical (infirmiers, aides-soignants, kinésithérapeutes, assistantes sociales, secrétariat),

- "Comptes génériques"

Dans un hôpital, il y a des postes fixes, et des ordinateurs portables.
Les postes fixes sont destinés :

- aux médecins
- au bureau du secrétariat
- aux postes de soins infirmiers
- aux urgences

Les ordinateurs portables sont attribués :

- aux infirmiers pour suivre les soins, administrer les traitements, faire des transmissions aux équipes en rotation nuit/jour,
- aux médecins pour prescrire des traitements et suivre le parcours santé des patients

Les quatre progiciels phares de santé sont :

- Ph***a, pour l'ordonnance et la commande/livraison de médicaments
- D***re, pour la gestion globale de la patientèle
- T**o, pour l'organisation du transfert et d'attribution de pôles aux malades
- Op**a, pour le suivi des opérations chirurgicales à venir, en cours, ou passées

Voilà sur le papier l'organisation.

## Ce que nous avons découvert, en pratique sur le terrain, est malheureusement effrayant :

**#Concernant les habilitations :**

- dans 90 % des cas, les utilisateurs des postes nomades ne verrouillent jamais leur session : il est fréquent qu'entre deux soins, une infirmière retrouve son ordinateur "emprunté" par une consœur, ou un médecin qui doit consulter en urgence le dossier d'un patient. La traçabilité est quasi inexistante.

**#Concernant les logiciels et progiciels :**

- 3 des 4 logiciels de santé utilisés dans ces hôpitaux ont des comptes génériques et communs à un service (donc login et password partagés et connus de tous), sinon ils sont simplement renseignés sur un post-it collé en bas de l'écran.

- Personne ou presque n'utilise de comptes nominatifs. La raison invoquée est le gain de temps : il est légitime et compréhensible qu'en urgence un expert de santé veuille immédiatement avoir accès à un planning de chirurgie pour réserver un bloc, ou prescrire un médicament précis, pour sauver une vie.

- 3 des 4 logiciels de santé n'ont pas d'expiration de session, ou alors quasiment : un seul à une expiration de deux heures, les autres peuvent tourner plusieurs semaines sous la même session sans discontinuer. Certains comptes que nous avons observés sont connectés depuis des mois, le/la propriétaire initial.e du compte ayant pourquoi pas changé de métier ou de secteur.

**#Concernant les postes (fixes comme portables) :**

- les clefs USBs et autres devices externes sont acceptés

- beaucoup de postes sont admin local de leur bécane, afin de ne pas entraver l'activité de personnel soignant pour un simple souci de "droits."

- aucune blacklist ou reverse proxy sur les sites consultables par les usagers (Facebook, sites de streaming et autres nids à RAT sont légion)

- les GPO ont été paramétrés pour désactiver la mise en veille des postes nomades. Comme vérifié auprès d'un chirurgien, pour accéder à un ordinateur de l'hôpital, il suffit de "bouger la souris."

- pas ou peu de NAC

**#Concernant la gestion des droits :**

Tous les profils, de la simple vacataire aide-soignante au chirurgien sénior ont un droit/devoir de consultation sur les dossiers des patients. Il nous a été répété de nombreuses fois que lorsqu'une personne "connue" ou célèbre est hospitalisée, son nom est largement et rapidement connu des employés de l'hôpital.

Ainsi, il apparait comme coutume de consulter par curiosité les dossiers médicaux de ces notables.

**#Concernant le processus de création de comptes :**

Dans la plupart des établissements de santé, la DSI est réduite à son strict minimum vital, approchant la mort clinique : les budgets et moyens humains ou financiers mis à leur disposition sont ridicules, leur fatigue chronique fait qu'ils outrepassent parfois les bonnes règles de cybersécurité (ajout de droits, pas ou peu de remasterisation des anciens postes, pas de vérification des attributions auprès des cadres), ou simplement qu'ils partent et changent de secteur.

**#Concernant la sécurité physique :**

Sur un des services observés, aucun changement du digicode protégeant des accès sécurisés depuis plus de 5 ans ! 8 ans pour le poste de soin (qui contient, entre autres, des stupéfiants, des tampons officiels, des ordonnances sécurisées, etc.)

En mode "red-team" nous avons pu, simplement dotés d'une banale blouse blanche, rentrer dans tous les services et pièces réservées strictement au personnel médical ultra qualifié. Sans aucune difficulté.

**#Concernant la sensibilisation :**

Les, je cite, "gars de l'informatique" viennent parfois éteindre les écrans ou verrouiller des sessions pour "montrer l'exemple". Ouch. Sinon, la Haute Autorité de Santé a mis en place un protocole d'audit, qui est en route mais absolument pas ni abouti ni concluant sur le parc français. On pense notamment à la double authent, qui se met progressivement en place.

Le but de cet article n'est absolument pas de tirer sur l'ambulance, vous me passerez l'expression. Sa finalité est de mettre en avant le manque CRIANT de finances dans ces pépites que la France a la chance de posséder.

Par exemple, sur le dernier service dans lequel nous nous sommes rendus, j'ai pu énumérer :

- 2 infirmières
- 1 infirmière référente
- 2 aides-soignants
- 5 étudiants

- 1 assistance sociale
- 1 diététicienne
- 1 cadre infirmiers
- 3 médecins externes
- 5 médecins internes
- 1 kinésithérapeute
- 2 infirmières spécialisées
- 1 infirmière pansements
- 2 internes visiteurs
- 10 chirurgiens
- 5 chirurgiens visiteurs

Soit 42 employés sur ce service.

**Savez-vous combien d'ordinateurs se partagent ils ?**

4 PC fixes et 3 ordinateurs portables.

8 ordinateurs au total ! Soit 0,19 poste par usagers…

Pour comparaison, 70% des enfants du primaire et du secondaires sont équipés par le gouvernement. Le taux monte à 100% pour les enseignants.

**C'est ce genre de chiffres qui semblent expliquer en grande partie la fébrilité cyber de notre système de santé.**

Dans toutes les sociétés où j'ai eu la chance de travailler, j'avais, à minima, un ordinateur de bureau, un ordinateur technique, un ou deux téléphones portables dernier cri, voire même une tablette. Une "abondance" dont je n'avais pas utilité.

Je vous laisse avec ces chiffres.

Mais aussi avec cette citation d'un philosophe :

« Plutôt qu'argent amasser, mieux vaut santé posséder. »

**La cyber guerre a depuis longtemps commencé, il est temps de faire rempart et de soutenir notre précieux et tellement envié système de santé.**

Des solutions d'excellence existent, je pense, à la volée à nos amis Darktrace, CrowdSec, YesWeHack ⁖, KeoPass, Yogosha et bien sur nous, le collectif Hackers Without Borders. Nous avons tous le moyen d'apporter une pierre à cet édifice qu'il faut renforcer de toute urgence.

Merci aux dizaines de chirurgiens, techniciens, brancardiers, paramédicaux qui ont bien voulu se confier anonymement et nous ouvrir les portes du cyber bloc opératoire. Il y a urgence.

PS : cet article ne fait pas de généralités, il recense simplement des faits qui ont pu être observés directement dans certains établissements. Il est évident que de nombreux hôpitaux peuvent avoir des sécurité largement plus robustes. C'est un article "cri d'alarme", qui se base sur des faits et d'observations, pour que plus jamais un ransomgang puisse mettre K.O un établissement comme Corbeil.

F.C

## **ANNEXE 2 :** Questionnaire à l'adresse des centres hospitaliers portant sur la perception de sécurité par les personnels soignants

Source : Nasir-Baba Ahmed, *Cybersecurity in Healthcare System: Evaluationand Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience*, thèse de doctorat en Sciences informatiques et cybersécurité, Institut des Mines-Télécom (IMT) d'Alès, université de Nîmes, 2022.

IMT Mines Alès
Ecole Mines-Télécom

**Questionnaire for MFH Users**

**Users - ALL/ANY**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | Do you worry about any cybersecurity attack striking this MFH? | Not very Concerned | Not Concerned | Indifferent | Concerned | Very Concerned | | |
| | | x | | | | | | |
| 2 | What type of cyberattack are you most concerned about? | Ransomware | Denial of Service | Compromised application | Insider Threat | Other(eg. Medical device compromise | Physical access/Intranet acceesss | Intelligence |
| | | | | X | | X | X | X |
| 3 | How confident are you in the MFH's ability to handle a cyberattack? | Needs an overhaul | Needs work | Adequate | Above average | Very Confident | | |
| | | X | | | | | | |
| 4 | Does the MFH have any dedicated information security staff? | No | No, but may hire in next 12 months | Yes | | | | |
| | | X | | | | | | |
| 5 | Does the MFH have a cybersecurity incident response plan? | No | No, but we plan to have it in 12 months | Yes | | | | |
| | | X | | | | | | |
| 6 | Has the MFH ever suffered from a cyberattack of any kind before? | No | Yes, in the Past year | Yes, more than a yea ago | I'm not sure | | | |
| | | | | | X | | | |
| 7 | Has the MFH ever paid a ransom or any extortion fee? | No | I'm not sure | Yes | | | | |
| | | X | | | | | | |

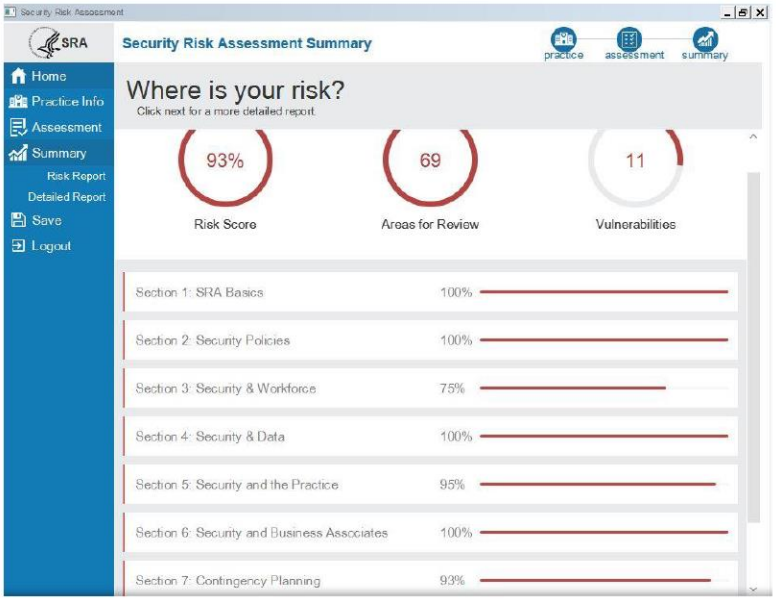
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8 | What do you think makes detecting any cyber threats difficult? | Lack of tools to monitor activities | Large number of users | More assets are on the cloud or off the network | Lack of staff competence on analyzing data permissions/access | All of the above | Emergency Situation - attention deficit |
| | | | | | | X | X |
| 9 | In your opinion, what are the major vulnerable activities or areas that are more likely to encounter a cyber attack? | Admin/ Reception | Triage | Xray | Hospitalization | | |
| | | X | | | | | |
| 10 | Do you think all the following stakeholders of the MFH are cyber-aware or trained? | Logistics | Physicians | Paramedics | Management | Other: | |
| | | | | | | X | |
| 11 | Do you think it is a time-consuming task to investigate or respond to cyber threats? | No | Yes | I'm not sure | Yes, but there is very little or no forensic capacity | | |
| | | | | | X | | |
| 12 | Regarding internal threats from employees or contractors, what are you most worried about? | Malicious users | Careless users | Compromised users | Other: | | |
| | | | X | | | | |

## *Suite du questionnaire :*

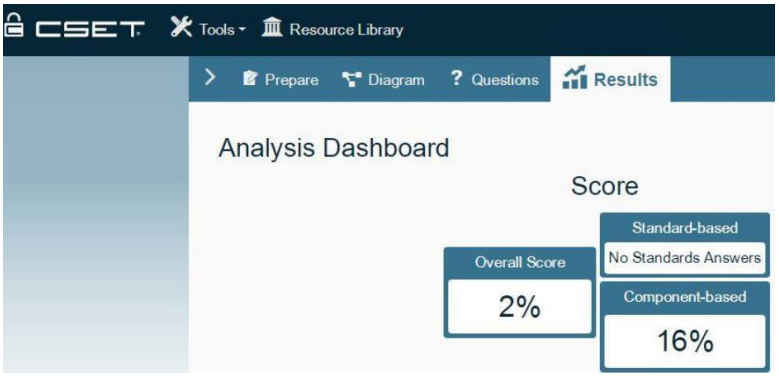
| | Users - TECHNICAL | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | What platform does the Computers' operating systems run on? | Linux | Windows | Mac | Other: Open office S/W | | |
| | | | X | | | | |
| 2 | Which Version? | 7 | | | | | |
| 3 | How frequestly is the operting system patched/updated? | Everyday | Every week | Every month | Every 6 months | Yearly | Other:No updates |
| | | | | | | | X |
| 4 | Which Network devices are deployed on the MFH for network distrubution/switching? And version | Mostly simple basic | | | | | |
| 5 | Which IP address assignment policy is implented? | DHCP | Static | Special/Custom | Other: | | |
| | | | X | | | | |
| 6 | Which device is deployed on the MFH for internet access? And version | D-Link | TP-link | Version: | | | |
| | | | | No internet Access | | | |
| 7 | Which password policy is being fully implemted to WiFi access? | WPA | WPA2 | WPA3 | 2FA | None | Other: |
| | | | X | | | | |
| 8 | Which email provider is being deployed/subscibed? | Hotmail/Live Enterprise | Gmail Enterprise | Yahoo Enterprise | Zimbra Enterprise | All personal | Other: |
| | | | | | | | NO |
| 9 | Which password policy is being fully implemted for PMR accesss? | Basic | Alpha-numeric | Alpha-numeric + Special characters | 2-Factor Authentication | None | Other: |
| | | | | | | | No password |
| 10 | Which method of managing/accessing patients records is implemted? | E-records | Physical File records | Both | None | Other: | |
| | | | | | | No Method | |
| 11 | What Patient medical record management system is deployed on the MFH? | Internally developed | Enterprise subscription | Other: | | | |
| | | X | | | | | |
| 12 | How is it Hosted for usage in the MFH? | Online | Local network | offline | None | Other: | |
| | | | X | | | | |
| 13 | Which password policy is being fully implemented for accessing PMR Records? | Basic | Alpha-numeric | Alpha-numeric + Special characters | 2-Factor Authentication | None | Other: |
| | | | X | | | | |
| 14 | Which records access policy is fully implemented in the PMR? | Role-based | Local Access Specific | Local Access Open | 2-Factor Authentication | None | Other: |
| | | | | X | | | |
| 15 | How often is the password change policy set? | Every week | every 6 months | Every year | More than 1 year | Never | |
| | | | | | | X | |
| 16 | Is the WiFi allowed to be used for personal use? | No | Yes | I'm not sure | No interenet, so no interest | | |
| | | | | | | | |
| 17 | Is the use of Personal WiFi hotspot allowed? | No | Yes | I'm not sure | Not with the PMR records, seperated and only for the HQ | | |
| | | | | | | | |
| 18 | Is there any medical equipment connected to the local network/internet? | No | Yes | I'm not sure | X-Ray | | |
| | | | X | | | | |
| 19 | Is there any policy for testing vulnerabilities in any medical equipments used on the MFH? | No | Yes | I'm not sure | | | |
| | | | | | X-ray only(Dcom) | | |
| 20 | What is the type of Barcode technology (Symbology) implemented ? | 2D Data Matrix | PDF417 | QR Code | Aztec | Maxi Code | 128 Linear |
| | | X | | | | | |
| 21 | Whtat is the type of Barcode reader used for scanning ? | Simple/old | | | | | |

***Grille de criticité et score du niveau de sécurité moyen pour les CH interrogés (1ère méthode d'audit) :***


***Grille de criticité et score du niveau de sécurité moyen pour les CH interrogés (2e méthode d'audit) :***




***Grille de criticité et score du niveau de sécurité moyen pour les CH interrogés (3e méthode d'audit) :***



# **ANNEXE 3 :** Déclaration de Robert D. Steele sur la nécessité d'un service de renseignement de sources ouvertes

**STATEMENT OF OSS CEO ROBERT STEELE**

*National Press Club, OSS-DNI Duel, 20 April 2006*

I am Robert David Steele—for the Latinos, my matronymic is Vivas. After a full career in secret intelligence, including responsibility for creating the Marine Corps Intelligence Command, I have spent the past eighteen years attempting to induce intelligence reform by drawing attention to the 80% of the information in all languages that our $60 billion a year secret intelligence community fails to address.

I have demonstrated repeatedly that 80% of what we need to know to make sound policy decisions, and to help our citizens and our Congress validate and hold accountable White House executives who claim support for their decisions from secret intelligence, is to be found within open sources of information that are legally and ethically available.

I have also demonstrated that the same 80% is not secret, not in English, not online, and not known to anyone in Washington including the Foreign Broadcast Information Service and its new cosmetic overlay, the Open Source Center at the Central Intelligence Agency.

I thought that we had succeeded in 1996 when the Aspin-Brown Commission, on the basis of the Burundi Exercise in which I beat the entire U.S. Intelligence Community overnight with six telephone calls, found our access to open sources to be severely deficient and recommended that it be a top priority for attention and funding. A succession of Directors of Central Intelligence ignored these and other recommendations, one reason why Senator David Boren, past Chairman of the Senate Select Committee on Intelligence, honored my first book with a Foreword.

I thought we had succeeded in 1997 when General Peter Schoomaker, then Commander in Chief of the U.S. Special Operations Command, and today the Chief of Staff of the U.S. Army, mandated that Open Source Intelligence be integrated into the Joint Intelligence Center and also into all of the Special Operations Forces schoolhouses.

I thought we had succeeded when Congressman Rob Simmons (R-CT-02), one of the early pioneers in this area, was elected to Congress and over time established himself as the go to Congressman for open source intelligence matters.

In each of these instances, from 1988 to 2006, I under-estimated the poverty of the intellectual and emotional resources available to those in the secret world. They literally refuse to acknowledge that their $60 billion a year secret world is accessing less than 20% of what is relevant and available, and in the process of losing most of it, producing less than 2% of what our varied levels of decision makers across all Cabinet departments require. I also under-estimated the lack of vision and integrity of certain members of Congress who persist in funding secret pork rather than common sense public capabilities.

The Director of National Intelligence is to be complemented for allocating $100 million to the Open Source Center, and for establishing the position of Assistant Director of National Intelligence for Open Source. The Director has also achieved a small victory in obtaining White House recognition of Open Source Intelligence as a separate discipline, despite fierce resistance from across the secret world.

Unfortunately, and I say this as a citizen and a patriot, $100 million for open source information and open source intelligence, in the context of a $60 billion a year secret budget, when it has been clearly demonstrated that less than 20% of what we need to know can be acquired by secret sources and methods, is lipstick on a dead pig. The Open Source Center and the Foreign Broadcast Information Service are the decrepit runts of the U.S. Intelligence Community, when they should instead be part of a larger independent Open Source Agency such as the 9-11 Commission recommended on page 413.

I and other have had to shed blood and labor for eighteen years to get to that recommendation on page 413, and yet the secret world refuses to acknowledge what I and a handful of others who equal me in knowledge have stated repeatedly: we need no less than 5% of the total budget, or in this case, $3 billion a year, for an Open Source Agency that is completely independent of the varied intelligence community organizations, and ideally under diplomatic auspices.

t must be under diplomatic auspices for the simple reason that 90% of what we need to gain from the open source world is not online, not in English, and not available without the collaboration of non-governmental organizations and elements of foreign governments as well as foreign private sector organizations that will never, ever, collaboration with a branch of the U.S. Intelligence Community.

The Director of National Intelligence is a well-intentioned and highly-qualified individual who has been straight-jacketed by the Vice President. It was Dick Cheney, as Secretary of Defense, who destroyed the Born-McCurdy National Security Act of 1992 that might have prevented 9-11, and it was Dick Cheney who helped make the 9-11 Commission a complete cover-up and white wash, undermining legislation and leaving the Director of National Intelligence a virtual eunuch with respect to the 85% of the national intelligence budget that is very inappropriately under the direct control of the Secretary of Defense.

I have decided, after eighteen years of persistent constructive efforts to help the secret intelligence community appreciate what open sources can do to protect America and contribute to America's prosperity, that I must now be more confrontational, a form of tougher love. I must demonstrate to the American people that the $60 billion a year we spend on secrets is a waste of money; that we can get a far better return on investment by starting first with open sources of information; and that only public outrage fueled by public understanding, will power this reform process.

I therefore challenge the Director of National Intelligence to a duel. An intelligence duel. He is free to draw on the entire $60 billion a year secret intelligence world, inclusive of the mediocre open source capabilities that he has marginalized. For each of ten questions, to be established by a public process moderated by an appropriate broadcast personality or personalities, for just one hundred thousand dollars per question, spread out over ten weeks I will demonstrate to the American public, to the DNI, to the White House, and to Congress, just how inadequate our existing national intelligence capabilities are, both secret and open, and I will demonstrate just how much can be done, at a trivial cost, when one actually knows what they are doing in the open source world, where one can leverage all information in all languages all the time.

It is my hope that the Director of National Intelligence will accept this challenge, fund it, learn from it, and use the results to demand that the Vice President back down and permit both the full integration of the national secret agencies under the Director's total authority, and also the immediate establishment of a separate Open Source Agency as a sister agency to the Broadcasting Board of Governors, under diplomatic auspices. It is my hope that this exercise—and the future benchmarking that an Open Source Agency will make possible across every

threat and every topic—will lead to draconian reform within the secret world, and in that way, will help make America a safer and more prosperous Republic.

We're not only not getting our money's worth, we're wasting valuable time. The Director and his Deputy know where to reach me. Thank you.

# TABLE DES ENTRETIENS

## Guide d'entretiens initial (abandonné rapidement)

1) Fonction, métier, structure/dpt d'appartenance ?

2) Quel rapport avec les SR ?

3) Rôle dans l'IE ? dans le renseignement d'État ?

4) Qu'est-ce que le « renseignement cyber » ?

5) Doit-on plutôt parler d'OSINT (ROSO) ?

6) Lien avec les techniques d'investigation des services de sécurité dans le cyberespace et VS la cybercriminalité et « cyberguerre » ?

7) Quelle place occupe ces techniques aujourd'hui par rapport au HUMINT (outils type ANACRIM…) ?

8) Quels liens entre privé et public/renseignement d'État/IE ?

9) Le RENS cyber, à travers l'OSINT forme-t-il l'articulation entre RENS d'État, IE et hacking ?

10) Si oui, quelles techniques, outils et méthodes sont communs avec la cybercriminels/hacktivistes/les hackers dits éthiques ?

    *L'observez-vous sur le terrain et dans le cadre de votre métier ?*

11) Idée d'une communauté de pratiques (in)consciente sur la base d'une uniformisation/homogénéisation des techniques de renseignement (hacking) et de cybersécurité ?

12) Quels liens entretiennent les services de sécurité au sens large avec les hackers (blancs, gris, noirs) ? De quelle nature, à quel degré ?

13) Les hackers sont-ils intégrés dans des projets de sécurité informatique ou des politiques de cybersécurité ?

14) Quels liens entretiennent les entreprises privées avec les hackers ? De quelle nature, à quel degré ?

Entretien 1

| | |
|---|---|
| **Nom** | **LEBERON Laurent (LCL)** |
| **Date** | 21/06/2017 |
| **Fonction** | Lieutenant-colonel commandant la Brigade de Renseignement de la Gendarmerie nationale (antenne Midi-Pyrénées) - Division des opérations |
| **Expertise** | **IE ; RENS** |

Entretien 2

| | |
|---|---|
| **Nom** | **LOEWENTHAL Jean-François** |
| **Date** | 26/06/2017 |
| **Fonction** | PDG de la société Intelligences (IE & investigations digital forensics), contributeur au CF2R. |
| **Expertise** | **IE ; RENS** |

Entretien 3

| | |
|---|---|
| **Nom** | **TONELLI Stéphane (ADC)** |
| **Date** | 28/06/2017 |
| **Fonction** | Adjudant-chef N-TECH de la Gendarmerie nationale (antenne Midi-Pyrénées) Section de Recherche. |
| **Expertise** | **IE ; Data Forensics/cybersécurité ; hacking** |

Entretien 4

| | |
|---|---|
| **Nom** | **PIOTROWSKI Jean-Nicolas** |
| **Date** | 03/07/2017 |
| **Fonction** | Chairman, PDG d'ITrust (société de conseil et d'audit en cybersécurité), Toulouse Labège |
| **Expertise** | **cybersécurité/hacking** |

Entretien 5

| | |
|---|---|
| **Nom** | **DOUSSET Bernard** |
| **Date** | 11/07/2017 |
| **Fonction** | Professeur des universités émérite, informatique, IRIT Toulouse 3-Paul Sabatier |
| **Expertise** | **IE/hacking** |

Entretien 6

| | |
|---|---|
| **Nom** | **CAZENAVE Damien** |
| **Date** | 24/07/2017 |
| **Fonction** | RSSI chez Vente-privée et précédemment chez Cdiscount |
| **Expertise** | **Cybersécurité/hacking** |

Entretien 7

| | |
|---|---|
| **Nom** | **PAPAEMMANUEL Alexandre** |
| **Date** | 26/07/2017 |
| **Fonction** | Directeur commercial Renseignement & sécurité intérieure chez Sopra Steria. |
| **Expertise** | **RENS ; IE** |

Entretien 8

| | |
|---|---|
| **Nom** | **HARBULOT Christian** |
| **Date** | 22/08/2017 |
| **Fonction** | Fondateur de l'Ecole de guerre économique de Paris et consultant. |
| **Expertise** | **IE ; RENS** |

Entretien 9

| | |
|---|---|
| **Nom** | **DESCHAMPS Christophe** |
| **Date** | 22/08/2017 |
| **Fonction** | Consultant/formateur en intelligence économique (veille/Osint). |
| **Expertise** | **IE** |

Entretien 10

| | |
|---|---|
| **Nom** | **GOMART Christophe** |
| **Date** | 23/08/2017 |
| **Fonction** | Ex-directeur (général) de la DRM et du COS, actuellement COO chez Unibail-Rodamco. |
| **Expertise** | **RENS** |

Entretien 11

| | |
|---|---|
| **Nom** | **TORRISI Christophe** |
| **Date** | 23/08/2017 |
| **Fonction** | Responsable sécurité économique à la DGGN. |
| **Expertise** | **IE** |

Entretien 12

| | |
|---|---|
| **Nom** | **TRUILLET Philippe** |
| **Date** | 15/09/2017 |
| **Fonction** | MCF en informatique à l'IRIT-Toulouse III, responsable 3e année en systèmes robotiques et interactifs, réserviste gendarmerie RCC |
| **Expertise** | **cybersécurité** |

Entretien 13

| | |
|---|---|
| **Nom** | **PERRIN Cédric** |
| **Date** | 05/10/2017 |
| **Fonction** | Ingénieur de contre-ingérence cyber à la DRSD. |
| **Expertise** | **Cybersécurité ; RENS ; Hacking** |

Entretien 14

| | |
|---|---|
| **Nom** | **CRASNIER Fabrice** |
| **Date** | 13/10/2017 |
| **Fonction** | Ancien Commandant la Division Analyse Criminelle et Investigations Spécialisées de la Section d'Appui Judiciaire (SAJ) de la gendarmerie, doctorant en informatique et membre de la RCC. Désormais chef Pôle Forensic à la SCASSI Toulouse. |
| **Expertise** | **Cybersécurité/cybercriminalité ; RENS** |

Entretien 15

| | |
|---|---|
| **Nom** | **Christophe.** |
| **Date** | 03/07/2019 |
| **Fonction** | Officier DGSI (DZSI Toulouse) |
| **Expertise** | **RENS-IE** |

Entretien 16

| | |
|---|---|
| **Nom** | **ODA Alexandre** |
| **Date** | 09/07/2020 et 16/06/2021 |
| **Fonction** | DevSecOps et hacker éthique (autoentrepreneur) |
| **Expertise** | **Hacking/RENS (ancien 13eRDP)** |

Entretien 17

| | |
|---|---|
| **Nom** | **HERTZOG Thomas** |
| **Date** | 14/06/2021 |
| **Fonction** | Pentester chez SecuLabs SA (Suisse) |
| **Expertise** | **Jeune hacker éthique/pentester/OSINT** |

Entretien 18

| | |
|---|---|
| **Nom** | **BAUZIL Yohann** |
| **Date** | 06/09/2021 |
| **Fonction** | Ingénieur informatique, chez Airbus Oneweb Satellites (SAS), Correspondant zonal de réserve de cyberdéfense adjoint (CZRA) - ZDS Sud au COMCYBER. |
| **Expertise** | **Cybersécurité (RSSI), ingénieur réseaux/systèmes** |

Entretien 19

| | |
|---|---|
| **Nom** | **CURTET Florent** |
| **Date** | 30/09/2021 |
| **Fonction** | Hacker éthique, expert cybersécurité/pentester à son compte |
| **Expertise** | **Hacking éthique, ancien black hat** |

Entretien 20

| | |
|---|---|
| **Nom** | **LEGAY Julien** |
| **Date** | 13/10/2021 |
| **Fonction** | Expert Threat Intelligence chez Sogéti. Ancien chercheur en physique et autodidacte en hacking. |
| **Expertise** | **Hacking, CTI** |

Entretien 21

| | |
|---|---|
| **Nom** | **« Bob » (anonymisé)** |
| **Date** | 15/10/2021 |
| **Fonction** | Chercheur en cybersécurité à l'ANSSI, hacker/OSINTer. |
| **Expertise** | **Hacking/OSINT/cybersécurité** |

Entretien 22

| | |
|---|---|
| **Nom** | **POUCHERET Victor-Louis ("doomer")** |
| **Date** | 14/11/2021 |
| **Fonction** | CTO BZhunt, hacker éthique |
| **Expertise** | **Hacking éthique/cybersécurité** |

Entretien 23

| | |
|---|---|
| **Nom** | **DOMINGO Clément ("saxX")** |
| **Date** | 15/11/2021 |
| **Fonction** | Hacker éthique franco-sénagalais |
| **Expertise** | **Hacking éthique/OSINT/cybersécurité** |

Entretien 24

| | |
|---|---|
| **Nom** | **DOUZET Frédérique** |
| **Date** | 30/03/2022 |
| **Fonction** | Professeur des universités (Paris 8-IFG) |
| **Expertise** | **Géopolitique du cyberespace, approche théorique des questions cyber** |

Entretien 25

| | |
|---|---|
| **Nom** | **METAYER Julien "Kermit"** |
| **Date** | 30/03/2022 |
| **Fonction** | Consultant freelance hacker "éthique"/pentester (basé à Lyon) |
| **Expertise** | **Hacking "éthique", pentesting, cybersécurité offensive** |

Entretien 26

| | |
|---|---|
| **Nom** | **EPELBOIN Fabrice** |
| **Date** | 08/04/2022 |
| **Fonction** | Entrepreneur dans le secteur numérique, enseignant du supérieur |
| **Expertise** | **Questions cyber, droits civiques, confidentialité en ligne, guerre informationnelle, hacktivisme** |

Entretien 27

| | |
|---|---|
| **Nom** | **KAZAR Yassir** |
| **Date** | 20/05/2022 |
| **Fonction** | Entrepreneur, co-fondateur et actuel directeur de Yogosha. |
| **Expertise** | **Cybersécurité, hacking** |

Entretien 28

| | |
|---|---|
| **Nom** | **SEJEAN Marc (interviewé par un de nos étudiants en école de journalisme, Tom Falguerolles)** |
| **Date** | 20/03/2023 |
| **Fonction** | Informaticien spécialiste en sécurité numérique. |
| **Expertise** | **Cybersécurité, hacking** |

Entretien 29

| | |
|---|---|
| **Nom** | **HAJRI Sylvain** |
| **Date** | 27/02/2023 |
| **Fonction** | Chef d'entreprise, co-fondateur de osintfr.com, communauté d'intérêt sur l'OSINT et fondateur d'epieos.com |
| **Expertise** | **Cybersécurité, OSINT, entrepreneuriat** |

Entretien 30

| | |
|---|---|
| **Nom** | **« Alice » (anonymisée)** |
| **Date** | 01/03/2023 |
| **Fonction** | Gestion de projet, entrepreneuse, développeuse blockchain, spécialiste de l'analyse de données et de la blockchain. |
| **Expertise** | **Hacking, Big data, OSINT, Blockchain, hacktivisme** |

Entretien 31

| | |
|---|---|
| **Nom** | **LAURELLI Olivier ("Bluetouff")** |
| **Date** | 30/03/2023 |
| **Fonction** | Journaliste d'investigation/Cofondateur de reflets.info ; hacker/informaticien autodidacte |
| **Expertise** | **Hacking, cybersécurité et confidentialité/privacy, OSINT, hacktivisme** |

Entretien 32

| | |
|---|---|
| **Nom** | **MANACH Jean-Marc** |
| **Date** | 10/04/2023 |
| **Fonction** | Journaliste d'investigation indépendant, spécialiste d'OSINT. |
| **Expertise** | **Journalisme d'investigation, OSINT, culture du cyberespace** |

Entretien 33

| | |
|---|---|
| **Nom** | **POUPARD Guillaume** |
| **Date** | 17/04/2023 |
| **Fonction** | Ancien directeur de l'ANSSI, directeur adjoint de Docaposte. |
| **Expertise** | **Cybersécurité & cyberdéfense** |

Entretien 34

| | |
|---|---|
| **Nom** | **LAMOURI Karim** |
| **Date** | 07/07/2023 |
| **Fonction** | Entrepreneur, consultant SI (ancien technicien/administrateur/architecte/ingénieur systèmes), président de Hackers without Borders (HWB) |
| **Expertise** | **Informatique, sécurité informatique, cybersécurité** |

Entretien 35

| | |
|---|---|
| **Nom** | **PENALBA Pierre** |
| **Date** | 07/07/2023 |
| **Fonction** | Policier à la retraite (chef de cellule cybercriminalité à la PJ de Nice), spécialiste de cybersécurité et de hacking. |
| **Expertise** | **Cybersécurité, cybercriminalité, hacking** |

Entretien 1

| | |
|---|---|
| **Nom** | **LEBERON Laurent (LCL)** |
| **Date** | 21/06/2017 |
| **Fonction** | Lieutenant-colonel commandant la Brigade de Renseignement de la Gendarmerie nationale (antenne Midi-Pyrénées) - Division des opérations. |
| **Expertise** | **IE ; RENS** |

Filière RENS GN (depuis 2 ans) : chargé de coordination RENS en M-P, en transversal avec les autres SR/la police.

- Ordre public
- Radicalisation
- Séco (« SECOPE » pour séco et protection des E)

Brigades GEND (→capteurs) de fonctionnement type DRM (données du terrain vers tête où on centralise)

**EMR** (état-major régional)

**EMD** (E-M dptmental)

**BT** (brigades terrain)

**DSSP SCRT DRSI (DGSI)**/ DGSE (rempart St-Et à Tlse) **AP (admin pénitent.) DRSD DIRECCTE**

*No way com avec eux*

**ENOPT** (état-maj opé de protect VS terro)

FICHIERS RENS de certains SR

**BDSP** (Base données sécu publique)

**FSPRT** (Fichier du traitement des signalements de prévention à caractère terro)

**CHRISTINA** (DGSI)

**RT DRSI AP**

(A Toulouse) ils se parlent.

**SDAO** (Sous-division )

➔ Section veille numérique (quand besoin RFI sur une personne)

**IRCGN**

➔ **C3N** (Centre de lutte VS criminalité numérique)

Le RENS cyber ?

Oui ROSO, ils font du SOCMint notamment.

➔ Sollicitation du C3N ou de la section veille numérique (SDAO), possibilité d'IS (interceptions de sécurité) sur cette base.

Les NTECH sont alors concernés (analyse de support, data forensics)

« *Tout est cyber maintenant.* »

« *Le cyber est le vecteur, mais la culture cyber, on ne l'a pas forcément [en France]. On y vient pour le renseignement.* »

Encore beaucoup de RENS humain.

« *On a dit souvent que la GN était maître dans l'art du renseignement. En fait, ce n'est pas dans le renseignement, mais dans l'information.* »

RENS parcellaire à la GN (c'est plus de l'info qu'il faut recouper).

La GN n'est pas trop non plus très sensibilisé au RENS.

« *Tout le monde à la GN peut écrire des conneries, il y a pas mal d'amateurisme dans les notes de rapports. Et c'est aussi le cas dans la Police.* »

Souvent : manque de fraicheur de l'info, et l'autorité adm n'est pas motrice (peu de suivi des individus).

« *Le côté cyber se perd,* alors même qu'il n'a pas encore été bien maîtrisé. » [probablement une remise en cause du fait de la dimension aléatoire du cyberespace]

« *1% de personnes radicalisées sont bien câblées. On a dit aux débiles d'oublier Facebook. Maintenant ils vont sur l'agence de presse de DAESH pour s'informer. Ce n'est plus vraiment sur FB qu'on voit les radicalisés. C'est dans le réel que ça se passe.* » [entendre il y a ceux qui maîtrisent le cyber (1%), et ceux qui sont ignorants et ne savent pas vraiment s'en servir + ceux qui n'y ont pas accès + ceux qui sont sensibilisés à revenir vers le monde physique.] Ca se passe aussi en partie sur des appli telles que Telegram.

Pas de cryptographie au niveau régional à la GN.

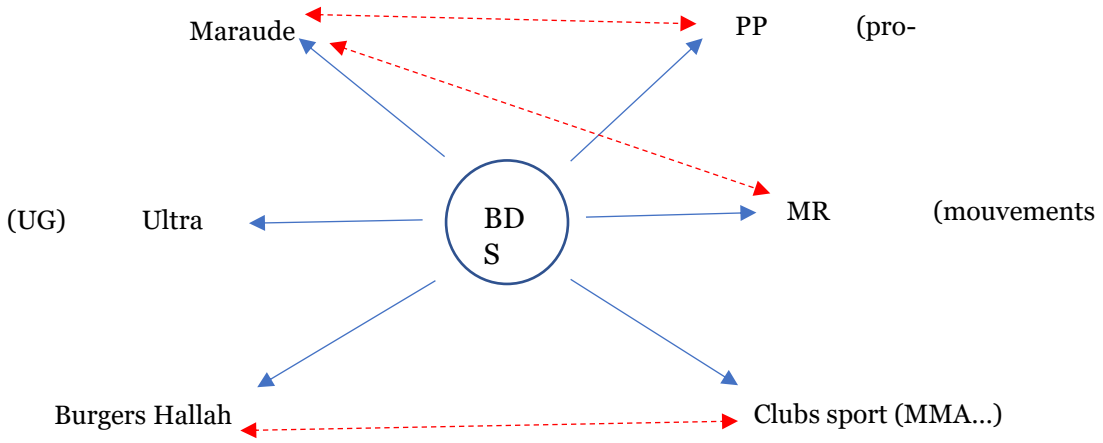
Anecdote contact avec la communauté juive locale (Tlse) qui vient au devant de la GN, le voir, et quel que soit le SR.

« *Ils crawlent le Web. Ils se revendiquent du Mossad ou en lien avec lui sans se cacher.* »

Ex. : ils le brieffent sur le BDS, un mouvement anti-israélien (notamment présent dans la propagande de boycott des produits israéliens.

LE BDS (*Boycott, Divestment, Sanctions,* ONG palestienne/propalestienne) a des connexions avec les militants pro-palestiniens

LCL Leberon fait le schéma suivant :




[Il pratique beaucoup/est fan du mind mapping // individuellement, car ses chefs ne font pas cas de ces méthodes d'analyse et de réflexion/débriefing. Ce n'est pas dans la culture des chefs. Mais lui a cette culture, pas forcément une question de génération. Ca a un impact.] Il pratique X-Mind.

---

Suite organisation environnement GN

Préfet

**GED** (Groupe d'évaluation départemental)

Hebdomadairement (Police, GN, AP)

**CDPR** (Cellule de départementale de prévention de la radicalisation)

Mensuellement (Police, GN, PJJ, représentant procureur Rép., profession santé)

« *En France, pour le renseignement, on n'a pas pris la mesure des enjeux*. […] *Il n'y a pas de culture du renseignement ou du lobbying en France*. […] *On a* [la France] *une myopie intellectuelle, pour tout*. »

« *Le renseignement cyber devient presque gadget. C'est une source, et cette source devrait être exploitée, mais devrait venir après le partage transversal de l'information.* »

Avec les nouvelles générations de cadres, c'est toujours pareil dit-il, ils sont prisonniers d'une culturelle institutionnelle.

Les nouvelles générations ne changent donc pas. « A la GN, il y a une consanguinité des chefs, qui sont tous saint-cyriens.

Même si ça change un peu (avec l'entrée d'universitaires).

A la police, ce sont les syndicats (très puissants) qui bloquent, et sclérosent les mentalités.

---

**Liens IE/RENS**

Système bicéphale public/privé avec les qualités et les défauts de chacun.

La DGSI utilise un système informatique US propriétaire (Palantir).

Notion de vitesse et de rentabilité pour le privé qu'il n'y pas (encore vraiment) dans le public.

| | |
|---|---|
| EMPS DIGITAL | 1 |
| TEMPS MEDIATIQUE | 2 |
| TEMPS POLITIQUE | 2 |
| TEMPS ADMINISTRATIF & JUDICIAIRE | 10 |

Dans le public, il y a une prudence qu'il n'y a pas dans le privé. La place du public est assujettie au politique.

« *Le temps* [les séquences liées aux évènements] *dépend à mon sens de l'américanisation de la société*. »

Avec Macron // c'est retour à VGE.

Mettre les chefs d'administration en position de responsabilité.

Les jeunes ne sont plus dans le HUMint, ils veulent tous faire de la veille, monter des cabinets d'IE.

**LCL LEBERON fait une veille perso sur Twitter (comptes des responsables politiques locaux)**

« *C'est le minimum. Mais, au-delà, je vais les rencontrer. Je vais au contact des politiques.* […] *Quand je peux leur rendre un service, je le fais…* » → HUMmint

Internet doit permettre de confirmer.

***« Il y a une communauté de pratiques entre renseignement, intelligence économique, voire avec les hacktivistes, mais pas avec les mêmes résultats.* [...] *Le pivot, c'est l'ingénierie sociale.* »**

[Appellation programme dans la GN : « Grand projet d'intérêt inutile », à côté de programmes tels que les radicalisations politiques/mouvements sociaux du genre Sivens.]

Dans ce cadre (surveillance de ces mouvements), LCL Leberon dit qu'il exploite l'info via SOCMint + HUMint : « *On voit les opposants en s'étant informé avant par le Web, au cours de stage de désobéissance civile qu'ils organisent par exemple. J'ai fait de l'ingénierie sociale.* »

La source cyber est une source intéressante qui vient en appoint. Elle est éclairante mais pas anticipative. Elle est nécessaire. Mais ne remplacera pas l'humain selon lui. Donc le partenariat, la logique public/privé continuera.

[Lubna BRIOUAL], perso dans le paysage toulousain… Contacter ?

**LCL Leberon répond affirmativement à mon hypothèse. Oui, tout le monde fait du renseignement en particulier via le Web [en tout cas de l'OSINF], au niveau perso et pro. Car, d'abord, on cherche des infos en amont pour connaître les gens, c'est devenu un réflexe.**

Par ex. le recruteur sur le plan pro.

« *On ouvre les vannes sur les RS, dans la sphère privée c'est déjà avéré.* »

//image publique que l'on renvoie (identité numérique)

Et notion de « double digital ». Il y a une connexion.

« *On travaille plus sur la personne que sur la donnée. C'est revenir à la source et pas à la donnée pour elle-même, ce n'est pas le contenu, le discours qui compte mais son auteur.* »

***« L'ingénierie sociale c'est le pivot, et le renseignement se fait à partir de la notion de double digital. »***

Les faux profils de GEND marchent pas mal selon lui. (surtour VS pédophiles et un peu VS les radicalisés ». Ça prend du temps.

Dans le paysage délinquant, il y a une population qui n'a pas accès à Internet toutefois.

« *On donne une place importante au digital. C'est le sens de l'Histoire.* »

La GN a recruté pas mal d'informaticiens sur titre.

**La GN a été la première à utiliser l'open source en France.**

**Une avance sur la police** selon lui, qui utilise des outils sur étagères.

C'a lui a apporté pas mal d'autonomie (mais parfois des problèmes d'incompatibilité avec les SI des autorités administratives nationales).

**BILAN-CONCLUSION**

Souci culturel - franco-centré

Pas de dimension européenne dans le RENS // avec lobbying.

En matière de cyber, on n'a pas été fort (car pas de lobbying)

- Faible culture du digital
- Et en même temps on s'éloigne du HUMint.

**« *Un pivot est en train de se créer autour de l'ingénierie sociale.* »**

Et le monde digital transpose les segmentations qui existent déjà dans le monde « physique ».

« *L'humain restera, que ce soit en physique ou dans sa déclinaison en 1 et 0.* »

« *C'est l'humain qui détermine la donnée ; et dans le RENS avant de travailler sur l'info, il faut travailler sur l'humain.* »

« *Risque principal : donner de la valeur à la com gadget.* [...] *La com, c'est la dictature de la pensée.* »

Le format Twitter est révélateur dit-il.

Autre risque, en ingénierie sociale, on peut se faire une fausse idée d'une personne. Danger du bais cognitif lui dis-je, il acquiesce. Danger du biais de confirmation. Donc les services publics doivent garder leur caractéristique du temps de réflexion, du temps long (difficile).

[Anecdote : LCL Leberon parle de Gérard Colomb, ministre de l'Intérieur depuis juin 2017. Il l'a cartographié rapido et a vu ses liens avec la police (un fils commissaire, etc.)

Il a « social ingénieré » à chaque fois par rapport aux politiques dont il dépendait : il en a tiré des modes de surveillance lorsqu'il était en charge de la sécurité routière (points de sécurité/contrôle alcoolémie)

Car les politiques passaient par là à telle heure, etc. A la question :était-ce volontaire de sa part d'analyser ces rapports et d'en user en influence, en choisissant les lieux et moment de contrôle, il répond « pas du tout », en souriant ironiquement.]

**Il parle de « social engineering appliqué »** [pas sûr que cela soit pertinent, puisque « cartographier » est une chose, qui reste théorique, alors que l'ingénierie sociale, c'est une manœuvre, c'est de l'action...]

Il en tirait, dit-il, un « avantage concurrentiel » (//police). En regardant où se trouvent les intérêts de chaque acteur.

**L'info est-elle = au RENS ?**

Non, l'info est le côté lumineux (un point de vue), éclairé des choses. Via la com par exemple, il y a un part de la vérité. Alors que dans le RENS, on essaye d'avoir tous les points de vue (*le clair+l'obscur* en qq sorte) [c'est moi qui formule ça, sur la base de sa métaphore].

FIN – il me donne un contact : Christophe TORRISI (DGGN Paris, spécialiste/coordonnateur de l'IE au plan national).

Entretien 2

| | |
|---|---|
| **Nom** | **LOEWENTHAL Jean-François** |
| **Date** | 26/06/2017 |
| **Fonction** | PDG de la société Intelligences (IE & investigations digital forensics), contributeur au CF2R. |
| **Expertise** | **IE ; RENS** |

Cabinet depuis 2001. (clients grands comptes – directions juridiques/sécurité). A été réserviste au COS.

Ses activités : IE/investigations (aspects concurrentiels, et criminalité économique ; « digital forensics - ~ data forensics, criminalistique technique).

A travaillé chez DCI (Défense conseil international)

Définition de l'IE (il dit qu'on ne parle presque pas d'IE dans les entreprises et le privé) selon lui : c'est celle du client.
« *Ma définition de l'IE : c'est celle du client.* »

3) Rens cyber.

« *Il y a un filtre marketing des définitions.* »

Les intérêts de certains groupes d'experts ou nouvelles administrations (voir de certains organismes étatiques // USA). C'est le fruit de / ça donne lieu à des guerres intestines.

Ex. : dans l'analyse du RENS avec par exemple le concept d' « *activity-based analysis* » (cf. NGA américaine). Une forme de concept marketing donc. Pas forcément non pertinent, mais dans une logique clairement communicationnelle.

CYBint

Threat intelligence …

Pas mal de concept d'origine US.

L'OSINT peut être considéré comme du renseignement documentaire.

Mais dans le jargon pro des SI (/SSI), on parle aussi d'OSINT. J-F Loewenthal me dit que dans le hacking/le milieu SSI, on utilise beaucoup ce terme en lien avec les phases de collecte (reco)) et avant la social engineering.

Donc OSINT doté d'une définition technique. Pour le cyber, milieux techniques.

Sinon, plus largement avec les cabinets d'IE… (c'est aussi le vocabulaire des cabinets d'IE)

**[Il y a comme un effet de mode à ce que l'OSINT/ROSO se résume au cyber]** : il confirme.

Ou c'est le fait des circonstances. Si tout se fait sur le cyber, alors logiquement… c'est là que ça va se passer.

[Il y a toutefois un aspect communicationnel important.]

Les greffes de tribunaux de commerce (infogreffe, société.com…) il faut aller chercher physiquement l'info (mais bon ça se digitalise…)

Les deux se mélangent… aspects coûts. Les sources ouvertes non numériques et les numériques.

L'OSINT, c'est de l'info blanche et grise.

JF Loewenthal pense que l'OSINT s'arrête en revanche à des communications/des informations normalement peu accessibles (communications téléphoniques, entretiens oraux…) contrairement à certains experts US (SCIP par exemple), qui estiment que même un entretien physique ou tél. fait partie des sources ouvertes, tant que les interlocuteurs spécifient leur identité, etc. //JFLoewenthal en parle dans son article CF2R.

[à mon sens, cela dépend en pratique de ce qu'en font les intéressés. Si par exemple, cet entretien se retrouve dans une thèse où les protagonistes sont désignés nommément, alors cela peut être légalement bien que moins ouvertement accessible au public. Si ce n'est pas confidentiel et/ou si c'est public (fond archivistique universitaire, thèse publiée, online…), alors ça reste de la source ouverte].

---

Forensics pour analyser les cyberattaques : mélange de threat analysis et de rétro-ingénirie.

➔ Pour avoir des bases de signatures, puis chercher sur source ouvertes.

On est ici dans le réactif (post-mortem en forensics, par analogie médicale).

Dans le défensif aussi.

Et aussi en amont → faire un peu de recherche ouverte (adresse IP…), et au-delà pirater des pirates, collecter soi-même de l'info. Assimilé à du « préemptif. »

Questions juridiques : pas de « légitime défense cyber » [la question est importante, il faudra y travailler]

11) On a le même environnement technique.

« *Les bons, en défense, doivent connaître les mêmes outils que ceux des attaquants.* »

Après, c'est une affaire de choix étatique ou personnel [individuel ?]

On a les mêmes techniques. « *La frontière n'est pas technique.* » [je parle de frontière juridique, légale, oui dit-il,] c'est la frontière juridique qui change.

5) CYBint // HUMINT : Complémentaire. Et il faut espérer que ce le soit. Dans une logique de complémentarité saine.

Il dit en substance : je peux utiliser un intermédiaire (en HUMINT), même si je n'en fais pas, et travaille sur le Web.

**L'open source est nécessaire en amont. [même conclusion que le LCL GN LEBERON]**

**Même dans le domaine militaire, on fait d'abord de l'OSINT** [/OSINF] (il parle d'OPEX qu'il a réalisées comme réserviste)

**Il y a un réel continuum entre l'OSINT, le cyber et le réel/l'HUMINT.**

**Sans « ouvert » avant, on perd du temps, de la pertinence, de l'efficacité en aval.**

10) JFLoewenthal confirme l'idée sur la production décentralisé/démonopolisé du RENS.

--- Idée d'encadrer les sociétés d'IE/les professionnels de l'IE (plus ou moins strictement entendus) // dans le cadre de la loi de sécurité intérieure.

Guéguerre entre SYNFIE et CNAPS (Centre national des activités privées de sécurité) à propos de ce possible encadrement. Les agents privés de recherche seraient tenus de déclarer à la préfecture leur statut, pour les assimiler aux métiers des professionnels de l'IE.

Pertinent ?!

Alors que tout le monde et notamment dans le privé et l'entreprise fait de la recherche qui peut être assimilé rapporté à leur activité à (une production) du renseignement (économique en particulier).

Ca dépend aussi des métiers/des directions.

USA → on peut parler d'une logique offensive, de guerre économique, et donc d'un véritable RENS dur (dans les affaires, VS la contre-façon…)

Tout le monde fait plus ou moins du RENS. (avec ses ressources et moyens propres)

➔ La qualité de données changent (méthodes disparates aussi)

Notamment gap dans le domaine le data forensics (anecdotes : traitement des fadettes, info fermée par nature)

Ponctuellement on peut arriver à des résultats proches. Question de moyens. Savoir-faire opérationnel très pro dans les réseaux criminels, et donc pas possible pour tout le monde.

Difficile cohabitation du privé et du public selon JFLoewenthal.

Anecdote : il achète et importe pour sa boîte du matos de forensics : les douanes françaises font pb. Ils voient d'un mauvais œil ce matériel spécialisé et étranger.

Le terme « IE », encore une fois, selon lui, ne correspond pas vraiment aux pratiques. Il me donne l'ex. d'Intelligence Online qui vient de changer l'intitulé de son deuxième pilier éditorial (la rubrique IE devient « renseignement d'affaires »). La mention IE a disparu.

Les liens public/privé donc, n'ont selon lui pas l'air très développés, à quelque exceptions près ou ponctuellement. [c'est sûr que ce n'est pas comme pour les USA].

[Anacrim est un logiciel anglais racheté par IBM, JFL dit que c'est le Analyst's Notebook d'IBM.]

Entretien 3

| | |
|---|---|
| **Nom** | **TONELLI Stéphane (ADC)** |
| **Date** | 28/06/2017 |
| **Fonction** | Adjudant-chef N-TECH de la Gendarmerie nationale (antenne Midi-Pyrénées) - Section de Recherche. |
| **Expertise** | **IE ; Data Forensics/cybersécurité ; hacking** |

Section de recherche (SR) // DAIC (F. Crasnier)

2000's

N-TECH analyse données numériques

IRCGN (les « experts » de la GN)

- INL//C3N (Institut numérique… // Centre de lutte contre les criminalités numériques)

Ingénieurs y compris contractuels.

Le C3N a été créé en réponse aux avancées de la police en cyber.

200 N-TECH aujourd'hui au niveau national.

Toujours sous-évaluation du politique par rapport aux moyens requis (2 N-TECH à Toulouse !), le numérique est dans toutes les enquêtes (stups, crim - téléphonie, emails…)

---

Donc cœur de métier : la data/le digital Forensics. La criminalistique.

Deux volets en vertu de la normalisation (certifications… telles ISO 27000, etc.)

BDRIS (Brigade départementale de renseignement et investigation judiciaire)

- 2 CICN (Cellule d'investigations criminalistiques et numériques).

Pas de transversalité. Ce que déplorent les deux N-TECH dont S. Tonelli.

Aspects de coopération internationale (//affaire Zone de Téléchargement), jusqu'en Islande. Sur des enquêtes liées au cyber. Bon retex, puisque ça a fait connaître la SR de Toulouse.

Et déjà, une première affaire, liée à un plateforme Bitcoin non officielle. Ca avait fait le buzz et amené la visite d'une enquêtrice japonaise en cyber (travaillant pour le FBI)

(Les Bitcoins autorisés par Japon et la Corée pour paiement des impôts, etc.

Les Yakusa utilisent les bitcoins.

(Club REUSSIR, influent à Toulouse)

Cyber peu d'impacts [je ne vois plus de quoi il était question]

FOVI (faux ordres de virements) et ransomwares sont les menaces cyber majeures (cybercriminalité)

Cas réel [que me relate S. Tonelli] : combinaison/hybridation des méthodes (méthodo criminelle protéiforme) :

Intrusion physique (pour placer spyware sur SI/une ordi de tel personnel) en parvenant à entrer illégalement dans l'entreprise.

Avec les infos collectées → social engineering sur RS (SOCMint), jouant sur les propos publics d'une employée racontant ses déboires amoureux…

➔ Véritable enquête.

La GN de Toulouse veut mettre des sources humaines dans le cyber. (voudraient trouver notamment des contacts dans les milieux de hackers).

Traces numériques formelles et informelles sont exploitées

Ils utilisent des crawlers dans le web et le Dark Web.

Il y au niveau national (C3N // SCRC) un processus d'indexation du Dark Web.

Sur le Dark, c'est là qu'on trouve les techniques criminelles innovantes, pas sur le web surfacique (blanchiment d'argent…)

Les vieux briscards du grand banditisme eux-mêmes se sont mis au numérique et utilisent le Dark, la crypto (on a trouvé chez eux des tuto dans cette optique…)

Cyber Hack à Toulouse (organisé par ITrust, le 21/09/17)

Mêmes pratiques.

**GRAPH SEARCH FB** en version English US, c'était hyper intrusif, lancé en 2013 [en réalité, il a été désactivé même aux USA en 2015 – il avait été empêché déjà en France par la CNIL], remontée via les tags hyper précise.

FB était (mais reste dans une certaine mesure) un vrai moteur de recherche, puissant.

Les journalistes l'utilisent énormément. Ils cherchent notamment de la data sur les hommes politiques.

S. Tonneli parle aussi de « FB stalker ». En fait, c'est **« StalkScan »,** une appli web indépendante opérant à parti d'un compte FB logé des requêtes prédéfinies (possibles directement sur le Search de FB) Tout ça reste comme le Graph Search (d'avant ou d'aujourd'hui) opérant à partir des publications publiques (donc les paramètres security/privacy fonctionnent et verrouillent)

Le volume d'info est énorme quoi qu'il en soit via l'OSINF → RENS [en réalité INFO] mais peu d'analyse.

« Les logiciels, c'est bien, mais on ne sait comment ça marche. » [parle de la France]

Evoque les failles d'un point de vue juridique/judiciaire. Du côté des autorités // la défense (avocats) peuvent démonter le travail des gendarmes.

[Cela rejoint ce que disait JF LOEWENTHAL qui évolue aussi (mais dans le privé) dans le digital forensic.]

Les enquêteurs doivent donc faire beaucoup de pédagogie (vulgariser), justifier, prouver pour la justice.

Emmanuel LEGRAND (espèce de « cyber-magistrat »), l'un des rares magistrats en France à être expert des TIC.

« *Le cyber prend le pas sur le « physique » dans les enquêtes classiques. C'est lié à l'usage qu'en font les criminels.* »

Ex. : un cas de viol → perquisition de nature numérique. Ca montre que les éléments numériques deviennent très importants pour les magistrats.

---

« Cybersextorsion »

Nigérians/RCI deviennent pro (du phishing après les débuts amateurs), mais aussi désormais dans la cybercriminalité/la « sextortion ».

Réserviste roumain, Servan Iclanzan, ancien légionnaire, et patron de la Gazette du Midi de Toulouse. Elu LR.

(Isabelle Lhermite (intégrée dans la réserve IE de la GN M-P ; il y aussi des gars d'Airbus)

La GN – les N-TECH aimeraient donc avoir des liens avec des hackers. Ils les suivent, recherchent des sources, mais c'est très encadré juridiquement (ou le serait s'ils arrivaient à trouver des indics dans le milieu)

Il mentionne Giorgia Masilotti (Toulouse, thèse cyberpédo), italienne en rapport expertise avec la GN.

Mention d'un Master « Ingénierie, sécurité, défense à Toulouse 3.

Entretien 4

| | |
|---|---|
| **Nom** | **PIOTROWSKI Jean-Nicolas** |
| **Date** | 03/07/2017 |
| **Fonction** | Chairman, PDG de ITrust (société de conseil et d'audit en cybersécurité), Toulouse Labège. |
| **Expertise** | **cybersécurité/hacking** |

Enjeu aujourd'hui : l'agrégation de données.

ITrust : infogérance de sécurité informatique

Collecte d'info/données + info acheté (BdD) + info informelle (Dark Web/auprès de Hackers)

Mais pas de flux automatisés avec les hackers par exemple (ou les autorités RENS/sécope locaux) → contacts ponctuels.

Mais travail de veille cybersécurité chez ITrust (signaux faibles, info sur ses entreprises clientes dans le Dark Web)

➔ Threat Intelligence

Fait nouveau aujourd'hui : le recours aux hackers mercenaires (pour le compte des États et d'entreprises)

**Selon lui,** pas les mêmes méthodes employées par ses équipes et les hackers [pirates ?], pas d'exploitation des failles, contrairement à eux (pirates. **[il ne fait pas vraiment la différence. Il a une vision très conformiste avec éthique et cie : sans doute dû à l'image qu'il veut conserver].**

Donc pas exploiter mais identifier les failles.

Pas d'exploit pour ITrust.

Il travaille (travaillait) avec la DGSI/DRSI Occitanie, qui eux font de l'exploit, mais à des fins surtout de sensibilisation.

---

RED TEAM

- Sur audit |intrusif
  | de code
- Analyse Dark Web
- Formation

BLUE TEAM

- Défense
- Développement produit avec équipe IA.

Le recrutement est classique chez ITrust (pas de hacker autodidacte, des profils issus des formations informatiques.

« Ça commence à rentrer. » évoquant la prise de conscience des entreprises // cybersécurité.

ITrust gagne un ou deux clients/mois (PME notamment).

12) Le terrain est élargi (par le cyberespace).

La manipulation mentale reste la même technique, ça n'a pas changé. C'était déjà ça avant (le cyberespace).

Plus d'infos à trier, plus d'outils de collecte.

Les hackers se concentrent sur un secteur économique, et sous-traitent l'info/la donnée de masse en Chine.

C'est la globalisation des données qui change la donne.

**ITrust utilise aussi les SOCMint**

**Ils cherchent des données, des mots de passe (prise d'empreintes [footprinting], il évoque nommément le concept de hacking – dans la reconnaissance).**

Toutes les sociétés de cybersécurité le font.

**Affaire Ashley Madison** (la société/site de rencontre adultère) : c'est une base encore exploité par des cybercriminels (pas mal de chantage – deux suicides consécutifs [aux USA il me semble]). **Même ITrust vérifie dessus si leur client peuvent être concernés.**

ITrust utilise des plateformes d'agrégation de données (technique/parfois humain→SOCMint). Ils utilisent des SIEM (security informaton and event management system – permet d'agréger-corréler les logs…) avec IA → analyse comportementaliste.

Il parle de **« connecteurs »** (comme équivalent des capteurs), reliés à des **« corrélateurs »**. } via des API/Data mining/SIEM. Produits corporate protégé.

Ils travaillent sur l'IoT également.

Près de 800 règles de corrélation (algorithmique)

+

IA (style Anacrim-Analyst's Notebook d'IBM)

+

Dark Web et SOCMint

C'est l'avenir de ces métiers.

On ne peut se passer de l'humain toutefois. C'est pour gagner du temps et épauler l'humain.

On évoque la question de la souveraineté, et notamment de la souveraineté industrielle.

(il déplore que les solutions Palantir soient achetées par la DGSI. Alors qu'il y a suffisamment d'expertise en France dans le privé.) Lobbying US ? Intermédiaires français « à la solde » US ?

IL a d'ailleurs coupé les ponts avec la DGSI depuis.

Il y a une tendance [au sujet de la convergence de l'info fermée et de l'info ouverte], mais selon lui l'open data par exemple est limité (si l'on veut des données de la région M-P, on n'aura pas tout, etc.). L'open data administratif selon lui n'a d'ailleurs pas de plan économique.

Il y aura selon lui toujours de l'info fermée (et c'est la plus-value des SR).

Mais surtout sur l'info ouverte [l'OSINF], le privé (une société come ITrust ou autre) est plus efficace que les SR.

Le lobbying à l'américaine selon lui existe et affaiblit la souveraineté. (rappel de l'affaire Palantir/DGSI).

Affirme que les militaires de leur côté sont en partie tenus (« financés ») par l'influence US [l'armée est en fait vraisemblablement partagée entre le souverainisme et l'inféodation aux USA]

Développer des outils en interne pour les SR coûterait trop cher (R&D, temps de retard…)

Pb de stratégie industrielle d'une manière générale.

Ex : Programme STORM SHIELD (parefeu français racheté depuis par Airbus – filiale Airbus DS Stormshield Network Security) Les entreprises absorbées : Arkoon et Netasq qui avaient déjà racheté SkyRecon.

Rupture dans le cercle (économique) vertueux en général : les sociétés françaises qui ne peuvent pas exporter. Pas de stratégie… Pas de commande publique.

Fonds d'investissement US ou CISCO/IBM qui approchent les sociétés du genre ITrust.

La blockchain ne remplace pas une PKI.

En contact avec la GEND (il les prend au sérieux et les dit efficaces). Avec DGSI black out donc depuis Palantir.

L'ANSSI est « catastrophique » pour lui : elle débauche les ingénieurs des ITrust-like…

Lui et une soixantaine de boîtes ont fondé un cercle d'animation de l'écosystème de la cybersécurité en l'Occitanie : l'assoc PRISM ( ! à dessein) Les *Professionnels de l'Industrie et de la Sûreté du Midi.*

En lien avec la région…

A ma demande, il me donne les contacts Franck Lepecq (Aerospace Valley) et Jérôme Lephay (ingénieur cybersécurité Rockwell à Tlse).

Entretien 5

| | |
|---|---|
| **Nom** | **DOUSSET Bernard** |
| **Date** | 11/07/2017 |
| **Fonction** | Professeur des universités émérite, informatique, IRIT Toulouse 3-Paul Sabatier. |
| **Expertise** | **IE/hacking** |

Activité, son métier dit-il : analyste de données.

Analyses données sémantiques ; bibliométrie web, logs, presse, annuaires.

Ils ont à l'IRIT crée une plateforme (collaborative).

Collecte, croisement, graph, cartes géographiques, analyses factorielles.

La plateforme est ouverte au public (moyennant un compte/mot de passe)

L'IRIT est centré sur la R&D.

Il produit plus des smart data que du big data (travail de big data ponctuel toutefois, sur les tweets par exemple).

Métadonnées de brevets par exemple.

---

Veille technologique, propriété industrielle/intellectuelle), puis envoi au CEIPI (Centre d'études internationales de la propriété intellectuelle de Strasbourg)

C'est de l'IE

Travail sur BdD de brevets (chinois, US, etc.)

BdD Web of Science (brevets), base de données de brevets chinois (?)

Les Chinois tentent des contre mesures en cassant la cohérence des caractères : ils changent de place les caractères (ils coupent les mots clés). Mais les programmes de l'IRIT peuvent reconstituer cette cohérence.

Outils : crawlers en html, « re-formateurs »

Base code : Pearl, Python… Codes préétablis (des non initiés peuvent utiliser ces produits après un minimum de formation – anecdote : un documentaliste peut les maîtriser en deux jours)

Email extractor, HTTrack

Brevets SPTO

Ces outils permettent de produire des synthèses automatisées de données

On parle de la **NSA** et selon lui → indexation sémantique de tous les fichiers de disques durs par défaut (visible selon lui depuis 2001 – Windows-lecteur C (ou D…), propriétés, autoriser l'indexation…

Ca forme une back door matérielle, exploitée par la NSA, qui permet recherche sémantique par supercalculateurs via mots-clés.

Anecdote : les cartes vidéo (style Nvidia…) ont une grande capacité de traitement, pas forcément vidéo, mais aussi en les reprogrammant pour tout autre fonction (les hackers utilisent systématiquement ça, dit-il), comme le traitement sémantique.

On produit du RENS avec les smart data. Le Big data est en réalité superficiel.

---

Il y a les données qu'on cible, et les données qu'on a déjà.

Connaissance interne + externe

Les hackers procèdent de même : ils ont en leur possession des listes de mots-clés, fichiers, personnes, des algorithmes qui génèrent des mots-clés [type SEO ?] → et les communautés que forment les hackers s'échangent massivement.

(Exemple : nombre de publications scientifiques // à la population //au pays. Cela donne beaucoup de finesse, ce sont des critères peu pris en compte en général dans les analyses/les collectes de données)

L'IA. Selon B. Dousset, on en a encore pour 20 ans avant que l'IA remplace à peu près l'humain.

Il parle de son intérêt par ex pour l'affectation optimale (fonction algorithmique) -- utile dans la RH par ex. Cela permet d'ordonnancer. Il dit qu'Airbus souffre d'une mauvaise affectation optimale.

Hybridation des acteurs ?

L'IRIT a créé un site web (basé sur le travail du CERN) : atlas.irit.fr (années 90)

Sur lequel tout le monde se loguait (les SR internationaux), curieux des activités du labo. L'IRIT se surindexait…

Jean Guisnel en avait parlé à l'époque.

Les logs peuvent cibler tous ceux qui visitent le site. On pouvait alors imaginer une activité criminelle style pirate.

Du coup, ils avaient créé un faux site par-dessus le vrai, à la volée.

---

Question de la fiabilité de l'info sera de plus en plus capitale.

Black SEO dans Web of Science (par ex.) par les USA : ce site américain tronque l'indexation des travaux scientifiques (des brevets), les brevets US non évidemment, mais les Européens ou les Chinois, oui.

Guerre de l'info/désinfo.

Il évoque des techniques de formulation de requête (syntaxe) sur moteurs.

Pour chercher un stage, un poste pour étudiants (ex. donné), il parle de la syntaxe « mailto » pour récupérer des emails. Ca crée des liens entre personnes et sujets auxquelles elles s'intéressent.

Enregistrer page, puis utiliser « Email extractor », logiciel gratuit.

B. Dousset utilise aussi HTTrack (un crawler)

---

Propriété intellectuelle et nouvelle technologies (PIN) //IRIT/Paul Sabatier Toulouse.

Fait de l'agrégation de données pour recrutement.

Question des open data [je lui parlais de sources ouvertes…, il embraye sur les open data] : selon lui c'est le chaos dedans, il faut faire de l'IE dessus pour remettre de l'ordre.

---

Question du travail sur forums et réseaux sociaux pour les analyses d'opinion.

(Dousset avait travaillé sur les données sur hommes politiques)

Le contexte global autour d'un personnage pollue souvent ces analyses tendancielles d'opinion (favorables/défavorables). Il peut donc impacté négativement les personnes (par ex : un homme politique qui traine des affaires : a constitue un contexte qui du coup a un impact sur les tendances).

B. Dousser a eu a travailler avec une thésarde en médecine sur les criminels/tueurs en prison : à partir de l'analyse des discours, et sur la base de critères jaugeant les poly-névroses que certains avaient, on pouvait dégager les criminels vraisemblablement véritables tueurs en série.

Tout le monde n'a quand même pas accès à tout ce que les data scientists ont et font. Les outils de base sont accessibles, mais pas d'autres (par rapport à l'IRIT, outils maison ?)

Exemple sur une thèse de finance internationale. L'approche humaine, les critères d'analyse comptent davantage que les calculs purs des machines.

Un nom : Maxime Wavasseur, thésard toulousain, spécialiste de R

m.wavasseur@gmail.com

[je vois les noms de logiciels utilisés par B. Dousset :

- Visugraph
- Trétralogie2 - irit.fr] ?

[A la fin de l'entretien, je m'interroge sur la façon d'utiliser éventuellement mes données d'entretiens : comment produire des données qui mettent en perspective les interactions entre les 3 sphères d'acteurs que j'étudie ? Si je parviens à quantifier, concrétiser ces interactions sous forme quantitative, je pourrai alors donner à analyser à B. Dousset sur sa proposition.]

Entretien 6

| | |
|---|---|
| **Nom** | **CAZENAVE Damien** |
| **Date** | 24/07/2017 |
| **Fonction** | RSSI chez Vente-privée et précédemment chez Cdiscount. |
| **Expertise** | **Cybersécurité/hacking** |

Venteprivée.com : 4000 personnels.

Il est autodidacte, bidouille l'informatique depuis jeune.

D'abord responsable sécu chez Cdiscount

Il a un associé qui a une boîte d'audit/pentesting (Florient…), dénommée SRT, et avec il organise des événements hacking (Sthack).

Beaucoup de boîtes embauchent au mérite et pas forcément au diplôme (surtout les PME ; les grands groupes ayant plus de contraintes ou dans un schéma plus traditionnel)

Chez venteprivee :

3 sections cybersécurité :

- Une équipe de pentesters (cherchent et corrigent failles)
- Gouvernance sécurité (politiques de sécurité)
  Logique de KPI (Key Performance Indicator)
- Un SOC (outils utilisés : SIEM avec moteurs open source avec juste couche propriétaire)

Les SIEM sont très chers et sont conçus par éditeurs spécialisés (pure players) ou boîtes de cybersécurité, voire des marques d'informatique (HP…)

Marques de SIEM connues :

SPLUNK (pas trop cher),

LOGPOINT,

ELASTIC SEARCH (BdD (Big Data))

➔ Utilisation de bases de logs avec reformateurs/parseurs (parsing)
➔ Ensuite on fait des requêtes sur des événements

Venteprivee prévoit de constituer une base de 400 événements déclenchant une alerte sécurité.

(Pour éviter au maximum les faux positifs).

➔ Traitement et à chaque événement : plans de réponse.

Typologie évènements problématiques :
- Data leaks (détection transferts sur clés usb, etc.)
- Phishing
- Vol physique (et de données [proche des data leaks ?!]

Tout ceci permet de créer une base de connaissances.

Les logs sont capitaux, il faut donc un SOC aujourd'hui impérativement dans les boîtes de cybersécurité dignes de ce nom.

**Simulation attaques /défense comme dans une pure boîte de cybersécurité chez venteprivee.**

**RED TEAM // BLUE TEAM**

**Et même PURPLE TEAM** (les attaquants et défenseurs se tiennent au courant de leurs démarches/actions, contrairement à la configuration classique RED//BLUE.

La RED TEAM a pour rôle de faire des sortes d'audits/attaques. Ex : récupérer bases clients, vol argent, simulation vol physique aussi…)

BLUE TEAM (en défense, en aveugle // à la RED)

Damien C. fait aussi un peu de sensibilisation en interne (e-learning et un peu en présentiel (ex : auprès des assistantes de direction).

Les personnels sont invités également à faire des rapports d'étonnement.

---

Liens avec autorités

**Quant il était à Cdiscount, il l'était avec la DGSI, superficiellement** (eux cherchant systématiquement à obtenir de l'info mais ils n'aident pas vraiment).

La DGSI s'est intéressée évidemment à son association et à l'évènement qu'il coorganise (le STHACK) à Bordeaux – en avril) voir site web du STHACK.

**Liens aussi avec les N-TECH de Bordeaux, mais plutôt des échanges amicaux. Il dit qu'ils n'ont pas la réactivité qu'il faut, voire les compétences spécifiques, sauf pour certains aspects (correspond à la GN à Toulouse aussi, par ex. en block chain/bitcoin). Pour lui, c'est vrai de toutes les autorités étatiques en général.**

Les N-TECH ont été rencontrés sur le STHACK. Damien C. est allé jusqu'à leur donner des infos sur des « hacktivistes » (en fait des personnes liées à la propagande islamiste de Boko Haram, me dit-il). Suite à des défacements de petits sites de type chrétiens ou représentant l'Etat.

L'ANSSI : selon lui, ils ne sont pas mauvais, mais effectivement (comme le disait PIOTROWSKI) et selon les SS2I, ils assèchent le marché des ressources humaines en sécurité informatique (paient plutôt bien).

---

Venteprivée recrute partout à l'étranger : trop de concurrence à Paris notamment. Pour lui, le niveau en cybersécurité est en France globalement faible. Peu de très bons (surtout en hacking)

Dans le e-commerce, au sujet de la fraude, il a appris par expérience que les bons clients se monétisent chez les cybercriminels. La question de la fiabilité du client est importante, car plus il achète (est bon), plus il est fiable, et plus il intéresse les cybercriminels car ils sont moins surveillés par les boîtes – ils ne présentent pas de menace quant à la fraude) Par ex. si un client

commande et fait livrer ailleurs plusieurs fois à des endroits différents, ce type de choses [avec j'imagine aussi le mode de paiement], c'est suspicieux et donc ils vont les traquer /suivre de près.

**Quand il était à Cdiscount, il surfait avec TOR et donc aller sur le « deep web ». D'une manière générale, il se dit beaucoup de choses sur le deep/dark web, mais plutôt en termes d'astuces pour la fraude justement.**

**Site onions donc, dans forums. Mais pour une boîte comme la sienne, c'est trop chronophage car il faut sans cesse échanger et être en ligne (dans cet espace, c'est du win win et la confiance est difficile à gagner évidemment)**

Donc ils allaient chercher des sources et de l'info.

**MAIS en fait, c'est beaucoup sur le web normal où les brokers revendent des infos (par ex : sur les zero day attacks, qui s'achètent → par des entreprises notamment. Du style TippingPoint. Boîte (filiale HP) et produit (IPS). C'est assez transparent du coup. → hackers « gris » en quelque sorte.**

**Qu'est-ce qu'en font les boîtes ensuite ? là est la question.**

Est-ce qu'elles les revendent aux Etats ?

Au secteur privé (d'autres boîtes) ?

---

Il a un contact italien (un vrai hacker noir à l'origine → séjour prison dans les 90's)

Il avait piraté la banque d'Italie !

Il a une boîte de brokers qui revend des failles. Doit me donner ses coordonnées.

---

**L'hacktivisme, c'est de l'IE dit-il.**

L'ingénierie sociale

Vrai pivot entre les 3 sphères (rappelle les propos du LCL Leberon – GN Toulouse). On ne hacke qu'en faisant de l'ingénierie sociale selon lui (notamment phishing).

Faille humaine donc. Le phishing est une arme très efficace selon lui.

Il a essayé un test de phishing sur récupération login/mots de passe auprès des salariés de venteprivée. Un commercial s'en était chargé, se présentant comme un sous-traitant. Il me montre le montage vidéo (pour une sensibilisation interne, très efficace.) [Il ne peut pas m'en faire une copie car la boîte est citée, Cdiscount à l'époque et son propre nom]

Sensibilisé rapidement à des aspects techniques pour avoir l'air de fiable auprès des personnels, le commercial en question allait jusqu'à faire faire des lignes de commande sur le DOS de Windows par les salariés. Au final = 50% de réussite de l'ingénierie sociale !

Avait filmé aussi une pratique piggybacking (filmée, réussie avec à la clé un vol d'une liasse de documents estampillées confidentiels, l'utilisation de trois ordinateurs dont un non verrouillé et l'autre la clé token insérée ! Essai de Rogue AP (access point) également.

Entretien 7

| | |
|---|---|
| **Nom** | **PAPAEMMANUEL Alexandre** |
| **Date** | 26/07/2017 |
| **Fonction** | Directeur commercial Renseignement & sécurité intérieure chez Sopra Steria. |
| **Expertise** | **RENS ; IE** |

Mon sujet : bonne intuition de ma part selon lui. Me conseille de me focaliser sur le renseignement cyber. [ce n'est pas tout à fait mon sujet]

Le RENS dintérêt cyber ou d'origine cyber, c'est « bullshit » d'une certaine façon : ces notions n'ont pas de vraie définition et proviennent de l'influence US.

On confond cyber et technique. Quel processus métier cela concerne vraiment ?

Comment orienter les capteurs ?

Méfiance de la part du RENS d'Etat vis-à-vis de la notion de « cyber ». Car difficulté de l'appréhender : ça heurterait la communauté du RENS (cloisonnement entre industrie/privé et public).

La question à se poser selon lui : comment l'Etat a-t-il appréhendé le cyber ? //RENS.

Biblio : Attention, danger cyber, Aymerick Bonnemaison.

Entretien 8

| | |
|---|---|
| **Nom** | **HARBULOT Christian** |
| **Date** | 22/08/2017 |
| **Fonction** | Fondateur de l'Ecole de guerre économique de Paris et consultant. |
| **Expertise** | **IE ; RENS** |

Convergence entre les 3 sphères ? Interaction entre SR et IE, voire hackers ?

Harbulot fait le distinguo entre « contenant » et « contenu ».

- Sur le contenant : oui, convergence
- Sur le contenu : non, pas d'échanges du tout, selon lui.

Les opérateurs privés ne cherchant pas à communiquer leurs infos sur les méthodes d'attaques informationnelles [CH parle bcp de guerre de l'info, donc « attaque » est à prendre comme offensive relevant de cela].

Pas de confiance dans les SR, donc pas d'échanges en France

A l'inverse des communautés de hackers.

De leur côté, les SR ne s'intéressent pas aux modes d'action des opérateurs privés. Selon Harbulot, dans le privé : c'est l'économie des forces et des moyens qui prévaut. (différent du public/SR).

---

Intelligence Campus (DRM)

// Intellipedia

En France → des précédents (le CRAC de la DRM), avec notamment une cellule DRM dans l'EGE. Dans le cadre de laquelle beaucoup d'études de cas ont été réalisées.

Ex. : cas de la guerre de l'info.

Sur le cas de la journaliste française (France 24) qui « s'en était pris » à l'armée, vis-à-vis de l'action de celle-ci en Afghanistan (voir infoguerre.fr)

L'armée avait sollicité l'EGE (étude de cas présentée par l'EGE à la DRM via ladite cellule) pour lancer une opération de contre-influence à l'endroit de ladite journaliste. Celle-ci avait été pressentie pour son reportage pour le prix Albert-Londres, devait le vendre à France 2. In fine, elle n'a eu ni l'un ni l'autre et a du mal à s'en remettre, sa réputation ayant décliné ou ses « entrées » ayant été bien entamées.

Dans le cadre d'un milieu semi-ouvert, difficile d'avoir des échos de telle ou telle affaire. Car méfiance, difficile de faire confiance dans les SR. Harbulot cite l'affaire du réseau d'espionnage français des entreprise US dans les 80's. L'opération ayant été découverte et éventé auprès du FBI du fait d'une révélation venant de l'intérieur de la DGSE (sous Pierre Marion). Harbulot évoque le scénario de la taupe US (CIA, Léa Drucker) du *Bureau des légendes* (« acte manqué de Brochand » ? propose-t-il ; ou plutôt bonne documentation en amont sur le sujet ?).

Harbulot : comment cloisonner y compris au sein des SR, donc par exemple au niveau national au sein d'un écosystème semi-ouvert comme Intelligence Campus ?

Les échanges d'infos se font avec des anciens des SR, notamment de la DO (division des opérations, ex-SA-service action), reconvertis dans le privé.

Donc avec l'IE, mais de manière générale, dans les rapports avec les SR, le temps du rapport de confiance est très long.

Car les anciens optent pour des solutions « dures » (fruits de leur culture organisationnelle) → pratiques illégales le plus souvent. C'est donc [comme je lui fais remarquer] tout le paradoxe du privé d'aller chercher des anciens des SR, alors que l'IE en France est décriée voire rejetée.

➔ La théorie de la valeur valorise l'info noire, car les entrepreneurs se disent que c'est ça qui va apporter un avantage décisif (et non pas le travail besogneux et régulier sur sources ouvertes comme l'est la veille)

Mention des cas Technip et Airbus // Mediapart.

Harbulot : les USA sont très efficaces dans l'économie et la géoéconomie, bien plus que dans la (géo)politique internationale.

Les acteurs d'opérations clandestines (forces spéciales) ont une approche très pro (car pragmatique) et de haute valeur ajoutée. Même au sein de la DO de la DGSE, la différence d'approche est flagrante avec par exemple la DR (division renseignement), qui de fait sont déjà en rivalité en interne : la DR méprisant un peu la DO, du moins la traitant avec une certaine condescendance. La DO aurait selon lui une culture et un enrichissement singuliers (pratique, retex, capitalisation) (pour le ROHUM s'entend).

En termes de cyber c'est différent.

---

On retrouve toujours l'humain y compris dans l'économie.

L'EGE avait coordonné des labs avec EPITA (école informatique, groupe IONIS), ils travaillent de concert sur des études de cas. Le facteur humain évidemment dans l'ingénierie sociale (phishing). Les « techniciens » informaticiens d'EPITA ayant parfois des soucis, limité par leur cadre technique, alors que les étudiants de l'EGE éclairant les études de cas avec un autre regard, moins techniques et donc presque plus à même d'appréhender les questions d'ingénierie sociale.

D'où la question : comment (et qui) recruter les talents de demain ? Il y a un vrai « combat cognitif » en jeu (mot de Harbulot), c'est une polyvalence réflexion théorique, pratique technique qui semble être le profil à rechercher (culture G, ruse, intelligence au sens large, connaissance, en plus des savoir faire techniques)

Harbulot évoque « une mémoire opérationnelle »

- Les SR seront-ils tjrs utiles à l'avenir : toujours oui, car les mutations des organisations (entreprises et autres organisations) génèreront sans cesse des failles.

La faille ne sera pas que technique (informatique).

Le RENS d'Etat est de plus financé par l'impôt ! Il y a un cadre, des règles. Si/quant privatisation du RENS : quelles règles ? domaine trop mobile, soumis au « mercenariat » économico-mercantile.

Les limites du RENS français selon lui : les jeux d'alliance et d'influence politique au sein même de l'Etat, des institutions. Jeux très complexes. Ou les théâtres (d'intérêt, d'action…) mal maîtrisés.

---

**Il me parle d'AXIS où travaillent deux contacts potentiels : Frédéric Reynal, spécialiste cyber, et Nicolas De Rycke.**

Entretien 9

| | |
|---|---|
| **Nom** | **DESCHAMPS Christophe** |
| **Date** | 22/08/2017 |
| **Fonction** | Consultant/formateur en intelligence économique (veille). |
| **Expertise** | **IE, veille** |

Il évoque sans le nommer Liveumap, ou le même style d'applications. Comme « Géostratèges » également. Il évoque aussi un équivalent anglophone sur l'analyse (en particulier en GeoInt) grâce à des sources ouvertes recoupées.

Parle des métadonnées qui sont de plus en plus connues des particuliers (et pas juste de la NSA !) et qui fournissent bcp d'infos, ces aspects techniques qui deviennent de plus en plus familiers à ceux qui s'y intéressent [d'une manière générale, le hacking devient plus populaire, et avec lui ses techniques et son esprit].

Il dit qu'il y même désormais manipulation des métadonnées pour leur faire « dire » des infos erronées (désinformation).

- Il évoque deux de ses anciens clients (il vit souvent à l'étranger – épouse diplomate) : des banques-assurances par exemple l'employait pour former leurs enquêteurs maison, juristes, par rapport aux cas de fraude à l'assurance : particuliers (clients/assurés) tentés de faire jouer les assurances en mettant en scène tel sinistre…

Donc de l'OSINT pour vérifier la véracité des propos et de l'exposition des faits, qui relèvent d'aspects juridiques. Ceci permettant de corroborer (ou pas) les discours des clients.

//ex. de particuliers assez idiots pour évoquer leurs méfaits sur les RS (du coup → SOCMINT)

- Travail sur appli – de retouche vidéo, on l'on retrouvait des éléments (création d'inverse vidéo ou apparentés pour détecter des éléments graphiques sur une vidéo normalement invisibles).

Il me livre une autre anecdote (qui reste à vérifier) sur l'ancien du GIGN : Le Gorgu (celui de l'affaire de Nouméa dans les 80's), qui avait réalisé une sorte d'audit du ministère de la Marine en matière de sécurité physique [quelle époque ?]

Habillé en marin, il n'avait jamais fait l'objet d'un contrôle quelconque et avait réussi à subtiliser des ordinateurs dont il avait mis en scène (par une sorte de jeu de pistes) la « prise en otage ».

---

Me dit que les cellules IE sont mal estimées dans les grandes entreprises, parce qu'elles ont recruté souvent un ancien des SR. Or la direction des grands groupes privilégie ces derniers et le côté sensationnaliste [rejoint exactement ce que m'a dit Harbulot]

- Anecdote sur une grande école de commerce parisienne (sans doute l'une des 3 : HEC, ESCP, ESSEC) qui aurait (il y a une dizaine d'années) un ancien des SR, ceci amenant même à un procès initié par ses concurrents.

- Selon Deschamps, risque du modèle Intellipedia → risque de leaks (ça reste du numérique [encore une fois plus un risque humain qu'informatique]

- Cas du type « Robin Sage » en Israël (est-ce le dernier cas dont j'avais appris l'existence ? → « Mia Ash » ? Apparemment non, car ce serait non pas des Palestiniens derrière mais un groupe de hackers supporté par l'Iran.

Donc autre cas d'une « Robin Sage » en Israël, une soldate de Tsahal (un faux profil en réalité créé par des Palestiniens)

Deschamps, dans le cadre de ses missions de conseil / formation en entreprises est toujours supposé

faire de « l'espionnage industriel », preuve que les clichés sont tenaces.

Autre cas avec un de ses clients : le CICR :

Pour justifier l'envoi ou non de vivre et autres aides dans telle ou telle zone humanitaire.

Comment vérifier la véracité des photos qui circulent, les valider ?

Il avait préconisé l'utilisation d'outils de vérif météo (Wolphram [similaire à SunCalc, mais plus large].

Ensuite, par le traçage des tweets géolocalisés, par exemple au Mali (pendant l'opé Serval) (car à une période on ne savait pas trop ce que l'armée française faisait et où elle se déplaçait). Cela marchait très bien, car on pouvait avoir des preuves de la localisation.

Effectivement, il y a une banalisation des outils de recherche dans la société.

Justement, il y aura en effet une demande de plus en plus forte pour la transparence, mais les méthodes du RENS classique demeureront, comme celles des grandes entreprises [dans leur démarche d'analyse strat.]

Les GAFA deviennent de vrais acteurs de la géopolitique, souhaitant traiter la question terroriste par ex., ou du moins contribuer [suppléer les Etats probablement], avec leurs budgets et moyens colossaux [des micilices/des communautés de hackers par ex ?] un peu à l'image de certains groupes / ONG tels que les Anonymous.

FB revient en Chine me dit-il, par le biais d'un accord de filtrage et de maîtrise sur les logs par l'Etat chinois.

---

**Contacts :**

Olivier Ertzcheid (blog *Affordance.info*), MdC en SIC (qui fait autorité selon Deschamps). Contacté sur LI

Terry Zimmer (blog *intelligencesconnectées*)

Jean-Christophe Notin (bouquin sur témoignage d'anciens des SR)

Sébastien Gioria (expert OWASP, RSSI) – contacté sur LI (23/08/17)

Entretien 10

| | |
|---|---|
| **Nom** | **GOMART Christophe** |
| **Date** | 23/08/2017 |
| **Fonction** | Ex-directeur (général) de la DRM et du COS, actuellement COO chez Unibail-Rodamco. |
| **Expertise** | **RENS** |

Une fois arrivé à la DRM, il n'y avait pas de RENS cyber. (donc en juin 2013)

C'est surtout et en premier lieu la DGSE qui l'a développé et le développe : ~ 600 ingénieurs en informatique.

Mais les armées disent alors qu'il faut une « arme numérique » .

Retrait avec Puga (2008-2013) aurait dit « le cyber, c'est à la DGSE. »

Mais tout le monde a fait du ROSO.

GOMART : « *On était dans les bibliothèques paroissiales !* » le ROSO se faisait encore et quasi-uniquement sur base de documents papiers (production académique, presse…)

La DRM a ensuite acheté un moteur de recherche (il a oublié le nom) à une entreprise privée.

Le virage n'a pas été assez rapide selon lui. Il disait à l'époque qu'il ne voulait pas être exclu du développement sur le cyber rens.

C'est donc parti de cette volonté, d'où la création du CRAC (Centre de recherche et d'analyse du cyberespace). Cela a abouti à l'Intelligence Campus (bien que ce dernier soit centré sur le GEOint et l'IMint).

Il a monté le CRAC avec l'aide d'une ancienne officier de la DGSE, passée ensuite à la DRM : Sophie GRIEFFE (colonel) – sophie.grieffe@intradef.gouv.fr

L'une des questions était [et est toujours sans doute] : comment séparer RIC et ROC ? Il dit que c'est une question importante.

Et, de son côté, le contre-amiral COUSTILLERE a développé ses propres outils aussi.

GOMART disait à celui-ci : « *Mais tu fais du RENS !* » (cyber)

COUSTILLERE a fondé un centre opérationnel cyber (un B2/J2 dirigé en fait par la DRM) → pour le ROC.

Pour le RIC, c'est plus compliqué.

Intelligence Campus vient donc après pour dégager des algorithmes (intérêt pour l'IA) de collecte et analyse de données – pour tous types de RENS : IMint, GEOint, CYBint.

D'où la montée en puissance du CRAC.

Invention de « plateaux »

Gomart dit qu'il manque une NSA/GCHQ français.

Un conseiller de Sylvie Goulard (ex-ministre défense), André Le Sang-Pietri ( ?) milite pour travailler avec les Allemands. Mais Gomart dit qu'il y a déjà des acteurs en France.

Il évoque l'Ecole 42 de Niel. Ses étudiants se font approcher.

Ils sont sélectionnés via un test appelé « la piscine ». Il en garde donc quelques centaines sur des milliers.

Ca intéresse les SR.

Esprit de la DRM en cyber : ne cherche pas à « casser » (cracker) mais fait du ROSO y compris (fonction veille stratégique) dans le deep/dark Web.

Alors que la DGSE elle, est plutôt dans l'offensive et le hacking.

Test quand il était au COS :

Mélanger ROHUM et CYBINT/SIGINT : pour savoir par exemple comment se pluguer sur des caméras, détectées au sol par soldats et piratées/trafiquées (injecter fausses images…) par moyens cyber.

Donc, le cyber rens est indispensable mais insuffisant pour tout savoir selon GOMART. Mais excellente base. (d'un point de vue de SR du moins)

Il ne croit pas que l'IF n'existera plus (//transparence) ; les SR auront dont toujours leur place.

Anecdote avec Jean Guisnel qui avait réussi par « ROSO » (+ connaissances/culture du milieu militaire) à remonter des fils à propos de l'affaire Bastien Alex (pseudo de l'agent DGSE en Somalie et assassiné par les Shebaab)

L'Analyst's Notebook (Anacrim) d'IBM avait déjà été acheté par la DRM en 2000 !

**Convergence hackers//SR et travail (rappelle la convergence du contenant évoqué par Harbulot). Mais les hackers ont des communautés dynamiques.**

Contacts :

Bruno DRAN (sur LinkedIn), ancien DGSE/DRM

Bosse au concours des mines maintenant.

Eric BONNEMAISON (DGSE - actuel)

Entretien 11

| | |
|---|---|
| **Nom** | **TORRISI Christophe** |
| **Date** | 23/08/2017 |
| **Fonction** | Responsable sécurité économique à la DGGN. |
| **Expertise** | **IE** |

Comme Papaemmanuel, il me conseille de me cantonner au (cyber) RENS d'Etat.

Avoir un ancien des SR à la tête de l'IE dans une entreprise, c'est acheter un réseau avant tout.

Dénominateur commun IE/SR : vulnérabilité des entreprises au risque cyber. Donc, en gros le renseignement économique/la sécope.

Question de l'externalisation du RENS.

Décalage entre le monde du cyberespace et le monde tout court/le monde judiciaire.

La GN est plutôt un acteur généraliste du RENS (capteurs généralistes), les (autres) SR étant des spécialistes.

Le GN complète en fait les SR du 1er cercle.

Le ressenti des entreprises comptent : comment elles vivent leur rapport à la sécurité

// rapport entre SR et IE (GN notamment)

**Le rôle de la GN serait sans doute utile ici en complément de la DGSI (PME/TPE autour d'un cluster).**

JIRS (juridictions interrégionales spécialisées), une division cyber dans chaque JIRS.

Question de l'éthique/déontologie

Faux comptes réseaux sociaux utilisés. Est-ce les autorités peuvent s'autoriser d'utiliser ce procédé ?

SOCMint → en tout cas, la GN aujourd'hui le fait (lutte contre pédo-criminalité notamment).

Voir C3N, colonel Nicolas DUVINAGE

Entretien 12

| | |
|---|---|
| **Nom** | **TRUILLET Philippe** |
| **Date** | 15/09/2017 |
| **Fonction** | MCF en informatique à l'IRIT-Toulouse III, responsable 3e année en systèmes robotiques et interactifs, réserviste gendarmerie RCC(Occitanie). |
| **Expertise** | **Cybersécurité** |

Communauté hackers → marginal (par égo/cupidité, proof of concept…)

Le concept même de hacker, selon lui, est difficile à appréhender : le hacking, c'est du test radical ; disséquer les phénomènes, comprendre comment fonctionnent les machines, retro-engineering…

Comprendre la machine et son fonctionnement…

C'est d'abord un jeu.

On fait du social engineering, on établit les organigrammes d'organisations, on se sert des métadonnées et des moteurs de recherche. [C'est un travail d'enquête]

L'ingénierie sociale constitue en effet un levier important dans l'obtention d'information, dans le hacking.

***Petit manuel de manipulation à l'usage des honnêtes gens***, le genre de livre constituant une bonne source d'ingénierie sociale.

C'est effectivement le pivot entre tous les types de rens, selon lui.

***Persuasive technology***, bouquin de B.J Fogg (un peu vieux, mais significatif)

Hacking éthique : on a beaucoup d'infos aujourd'hui, mais (big data).

Leurre évidemment du tout-SIGint.

Rens cyber : écran de fumée ??

Le marketing, etc., c'est de la manipulation !

Des idéologiques hacktivistes/alter essayent de désintoxiquer de cette manipulation mais ils récupèrent les outils numériques et réutilisent l'info [et deviennent souvent une nouvelle intoxication, extrémiste, à l'envers → réinfosphère….]

On a trop segmenté en France entre disciplines (et donc en informatique/robotique/IA/SHS…) !

Pas d'interface entre elles ou alors ça vient trop tard.

L'humain est au centre, la technique n'est qu'un outil.

Question de l'auto-contrôle, sur wikipédia par ex.

GAFA et Etats : collusion parfois pour puissance et surveillance dans le cyberespace.

Pb de compréhension/d'interprétation (d'analyse donc des données/infos)

Infoviz (information visualisation)

Fourvoiement selon lui avec la question de l'IA (deep learning notamment) → faux positifs, faux négatifs…

L'humain sera toujours nécessaire, et son intuition sera très difficile à copier à l'identique si ce n'est la singer.

Ex : le modèle Anacrim → l'humain est toujours nécessaire. Anacrim reste un outil de mise en relation de données (qu'il faut sélectionner et « rentrer » dans le logiciel)

[Ce n'est pas de l'IA toutefois]

On veut, dit-il, à l'IRIT, pas de l'automatisé mais de l'informatisé. Donc de l'humain.

Logique de communauté dans la société pour intelligence collective pour régler des problèmes en tous genres.

Ça (re)crée du lien social, [paradoxalement]. Logique virtuelle à la base (communauté de gamers…), puis aujourd'hui reterritorialisation avec les Fablabs.

Le numérique recrée presque du lien social dans le contexte de leur délitement…

TOR

Principe d'anonymisation.

Lui ne fait pas la différence entre dark et deep web

« Warez » (fin des 1980's) : sorte de P2P où on s'échangeait des films, etc.

**Contacts :**

Guillaume CABANAC (Toulouse 3) analyse SOCMint

André Aoun

Abdel Malek Ben… (je l'avais contacté sur LI, pas de réponse) font des exos/simulation (pool) hacking.

Christophe Hurter (chercheur à l'ENAC en dataviz) – christophe.hurter@aviation-civile.fr

Frédéric Lenfant, ancien analyste Sogéti, et aujourd'hui chez Continental) Détection signaux faibles…

fred.lenfant@free.fr

Frédéric Stryjack (GN, a créé un centre de RENS VS radicalisme – à Toulouse ?)

Entretien 13

| | |
|---|---|
| **Nom** | **PERRIN Cédric** |
| **Date** | 05/10/2017 |
| **Fonction** | Ingénieur de contre-ingérence cyber à la DRSD. |
| **Expertise** | **Cybersécurité ; RENS ; Hacking** |

**DRSD :** mission de contre-ingérence de défense en renseignant (identification des vulnérabilités et détection des menaces) et protégeant (contre-mesures vulnérabilité et mesures d'entraves) à travers deux volets :

- Contre-ingérence des forces
- Contre-ingérence économique
- Mission transverse de cyberdéfense (contre-ingérence cyberdéfense) sur le cyberespace (recherche humaine et technique, sources ouvertes, investigations numériques ; liens avec CALID et ANSSI/les autres SR).

« Renseignement cyber » ?

➔ RIC et
ROC (le rens peut alors concerner l'IE, intéresser un personnel…)

Le ROSO (OSINT) est un des imputs pour le RIC et le ROC.

Acronyme TESSCo (propre à la DRSD) : l'ensemble des menaces qui pèsent sur le secret de la Défense : Terrorisme, Espionnage, Sabotage, Subversion (atteinte à l'image des forces armées et/ou l'état d'esprit des personnels), Crime organisé.

Hackers - IE – RENS

On ne s'intéresse pas au même niveau de l'internet selon qu'on est l'un ou l'autre de ces acteurs. Les hackers plutôt dans le « darkweb », l'IE plutôt au monde économique et de l'entreprise… Mais chaque niveau est perméable et l'on peut y glisser…

Le cyber : milieu unificateur ?

Oui ! **Un cyberespion utilise les mêmes techniques qu'un hacker** (y a-t-il une différence d'ailleurs entre les deux, puisque bcp de hackers sont des mercenaires qui peuvent agir comme tel ?)

Hackers//RENS

On cartographie les vulnérabilités, les points d'entrée, les exploits… (recon/footprinting…)

➔ Donc oui uniformisation des pratiques et des techniques.

Puis vient ensuite la technique, l'exploitation.

Objectif du hacker ?

Hacktivisme, crime organisé… TESSCo…

Cet acronyme sert aussi de matrice/grille de lecture pour appréhender les incidents cyber.

Parallélisme ROHUM C/R et le hacking (face au même type d'info : noire) : correspond bien en effet selon C. Perrin. (reconnaissance (R)/ingénierie sociale (C)).

**Selon lui, on peut tout à fait faire des parallèles entre réalité physique (des réseaux, etc.) avec les réseaux et infrastructures informatiques ; réseaux physiques/réseaux cyber.**

**L'humain demeure…**

Quid de l'ingénierie sociale ?

*Débat. Pas consensuel lors de l'entretien.*

D. Guiral (ne veut pas que cela apparaisse dans mes travaux) : il n'a pas la même définition (et selon lui il en va de même avec la définition maison DRSD du phénomène) de l'ingénierie sociale. Alors que C. Perrin (pourtant lui aussi DRSD) et moi-même ne sommes pas d'accord.

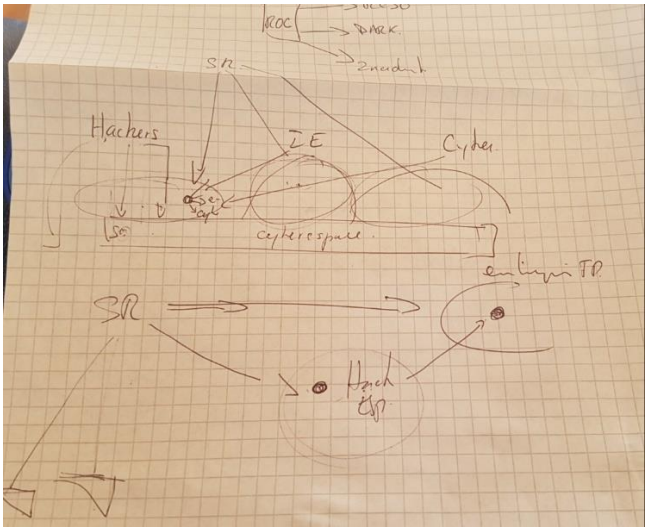
Il ne compte pas l'action de manipulation dans l'ingénierie sociale et résume ça au seul travail de préparation d'une attaque (avec prise d'infos…). Avec CP, nous pensons que c'est bien un ensemble : préparation, prise d'infos mais aussi attaque par manipulation psychologique, élicitation. Or, la GN et même les communautés de hackers parlent bien de manipulation mentale (Mitnick par exemple). Le phishing est d'ailleurs bien considéré comme un vecteur d'attaque par manipulation, influence néfaste proche de la tromperie/duperie/supercherie. Le phishing est bien de l'ingénierie sociale (prise d'info mais pas obligatoire, et manipulation, exploitation de vulnérabilités psychologiques)

Différences DARK, DEEP Web, Dark Nets… ? Pour lui, pour la communication, cela a du sens. Mais ramené à la technique informatique : pas de sens. Tout est une question de protocoles de communication entre infrastructures hardware, machines, serveurs (couche physique, liaison/réseau/transport…).

Existe-t-il des communautés de pratiques ?

Oui, il existe des communautés de connaissance, en termes d'informations par contacts étroits et interrelations entre hackers, entreprises pratiquant l'IE et les SR/RENS d'Etat. Mais il y aussi des communautés en termes de compétences, d'intelligence collective, en termes de ressources humaines.

IE-SR, SR-hackers, IE-hackers… (schéma de C. Perrin)



Tout en haut, « ROSO »

Brokers

**Les hackers sont souvent des intermédiaires, des sous-traitants, des mercenaires.**

Hybridation cybercriminelle comme dans le crime normal (hybridation des acteurs et des pratiques).

**Les hacktivistes conservent une sorte de code d'honneur** (du moins parce qu'ils se battent pour une cause).

Projet Intelligence Campus à la DRM : participe de cette mise en communauté (différents acteurs publics/privés, recherche universitaire/entreprise/Etat-autorités politiques….) Idée encore une fois d'uniformisation.

Il est aussi intéressant de noter que dans le cadre des tables rondes, conférences, sensibilisations grand public sur la cybersécurité, il y a toujours plusieurs communautés représentées (sauf « black hats » toutefois…)

Intellipedia (CIA, communauté du Rens US) : sans doute pas d'échanges d'infos notamment produit du RENS de chaque service/agence… Confirmation de D. Guiral.

En revanche, partage de pratique (ce que l'on voit dans le monde privé et de l'entreprise en fait). Donc, on voit bien la mise en réseau, les interrelations, les croisements, l'hybridation…

L'équivalent français est l'Académie du RENS, même s'il n'y pas (pas encore) la dimension numérique. Pas de plateforme numérique collaborative, mais site web.

Et existence d'un réseau interministériel avec partage d'info classifiée hors et avec SR (groupes de travail…)

A CREUSER (cela correspond-il avec ce que le gnrl GOMART disait : existence d'un réseau type interministériel mais dans une logique de lutte informatique offensive (ce qui était totalement secret – info noire. Gomart me précisant que c'était en off, concernant le contenu de notre entretien).

Quoi qu'il en soit, C. Perrin et D. Guiral sont unanimes sur la montée en puissance de l'Académie du RENS : expertises partagées, groupes de travail, networking, intelligence collective, partage d'état de l'art de certaines questions, thématiques dans leur travail respectif de rens…)

Ca ressemble (networking notamment) à ce que l'on fait dans le privé et le monde de l'entreprise.//société de la connaissance.

Plateforme Acyma (bien que pas en rapport avec le RENS)…

Selon C. Perrin, c'est la durée du secret de l'information/du RENS qui va muter : elle se raccourcira à coup sûr. Les secrets se dévoileront de plus en plus (idée de la citation de Racine) et assez vite. Mais seront quand même des secrets dans un temps donné : d'où la plus-value des SR à l'avenir encore. Ensuite, la plus-value du RENS d'Etat, c'est aussi le travail d'anticipation stratégique, le travail sur le temps long qui permet celle-ci.

Notion, approche de la cybersécurité, selon l'Etat français :

| **Cyber protection** | **Cyberdéfense** | **Cyber résilience** |
|---|---|---|
| SSI | Veille, alerte, réponse | PRI |
| Avant incident | Pendant | Après |

PRI = plan de continuité informatique (même chose que le PCA)

[CIRASCO, acronyme en lien avec crime organisé]

Entretien 14

| | |
|---|---|
| **Nom** | **CRASNIER Fabrice** |
| **Date** | 13/10/2017 |
| | Ancien Commandant la Division Analyse Criminelle et Investigations Spécialisées de la Section d'Appui Judiciaire (SAJ) de la gendarmerie, doctorant en informatique et membre de la RCC. |
| **Fonction** | Désormais chef Pôle Forensic à la SCASSI Toulouse. |
| **Expertise** | **Cybersécurité/cybercriminalité ; RENS** |

Fait la distinction OSINF/OSINT

RENS, oui les hackers et cyberdélinquants/cybercriminels en font aussi, car : il s'agit d'une contextualisation des infos (donc de l'info au RENS).

Hacktivisme…

Simplement, ils n'ont pas de règles // RENS/IE.

Cyberespace → « pot-pourri ».

[Aujourd'hui, c'est un peu du PUSH finalement, avec l'infobésité et les moyens de veiller – du moins en info blanche]. Mais avant on allait chercher l'info physiquement. Aujourd'hui on continue d'aller la chercher (info grise/noire), mais « on va chercher des bits » (dixit F Crasnier).

Il y a juste un changement de format, c'est tout. Les méthodes sont modifiées car nouveau support.

Possibilités infinies, décuplées.

Image du parallélisme entre cyberespace et espace physique [même idée que C PERRIN]

OUTILS

Technologie MERISE [vérif orthographe] qui sert depuis déjà plusieurs décennies à créer et gérer des BdD relationnelles.

C'est la technologie des **ONTOLOGIES** (analogie informatique avec la notion philosophique)

- ➔ BdD relationnelles très riches (Bid Data). But : ramener la sémantique et l'info. Les corréler. Produire de l'info grâce à la sémantique (sens créé par les relations, la corrélation de données).
- ➔ Contextualisation des données donc (corrélation).

C'est le WEB 3.0 (sémantique). C'est en fait assez ancien, mais ce n'était pas encore « connecté », hors ligne. Aujourd'hui, ces technologies, basées sur MERISE mais améliorées,

ces ontologies sont implémentées progressivement dans le WEB (le W3C travaille d'ailleurs à leur standardisation) pour faire le Web sémantique. Le moteur Google implémente peu à peu ces techno (la pertinence, les contextualisations, les interrelations sont de plus en plus performantes…)

L'idée du RENS produit par tout une chacun : oui

Car dilution dans la société (idée de la démonopolisation, décentralisation et désintermédiation du pouvoir, de la production d'info…) Le pouvoir se dilue, et donc l'information et la connaissance de fait. Transfert vers le pouvoir individuel.

Pas d'avis sur les « DARK NETS ».
Mêmes idées que P TRUILLE TOR, le DARK WEB, le DEEP.

Le DEEP étant bien tout le Web non indexé par les moteurs de recherche accessibles par des navigateurs WEB.

Je n'ai pas évoqué l'ingénierie sociale avec lui. Ou peu…

Entretien 15

| | |
|---|---|
| **Nom** | **Christophe.** |
| **Date** | 03/07/2019 |
| **Fonction** | Officier DGSI (DZSI Toulouse) |
| **Expertise** | **RENS-IE** |

Les dirigeants des SR ne se soucient pas du cyber selon lui.

Elément-clé : le stockage [Big Data ?]

L'humain est le + important.

Plus de coopération interservices

(N'est pas convaincu qu'il y aura une pénurie d'experts cyber techniciens à l'avenir.)

Sur le **cluster** Data Intelligence **du GICAT**, il ne dit rien, ni sur Palantir [que j'évoque] : il ne dit pas que ça ne marche pas, mais précédemment il a dit que la concurrence est incontournable. **Donc, mutualisation difficile**. Rien de bien neuf comme info.

Ca reste cloisonné entre domaines et secteurs d'activités.

Problèmes des actionnaires.

**Echanges/interactions entre entreprises et Etat en fonction de leur savoir-faire respectif. C'est là qu'il y a un réseau.**

Quand je lui demande s'il y a ces interactions Etat-entreprises et acteurs privés non institutionnels et informels (type hackers), il dit : « qui peut le dire ? »

Face à mon hypothèse (ces acteurs ne communiquent pas ou peu), il rétorque : « c'est votre hypothèse ». [Lard ou cochon, façon implicite de le confirmer ?]

En substance, il ne veut pas parler. **A rapprocher du témoignage d'Alexandre Oda.**

Il **me dit de me concentrer sur la communauté du RENS française [pour faire émerger des choses** a priori]

Entretien 16

| | |
|---|---|
| **Nom** | **ODA Alexandre** |
| **Date** | 09/07/2020 et 16/06/2021 |
| **Fonction** | DevSecOps et hacker éthique (autoentrepreneur) |
| **Expertise** | **Hacking/RENS (ancien 13eRDP)** |

Profil atypique donc : à 15 ans arrête la scolarité et armée (au 13eRDP) où il fait du RENS de terrain/de contact.

Forme en master secu réseau et infrastructure à l'ORT (sorte de CFA privé à Colomiers) où il avait été refusé plus jeune !

Estime que c'est vers 2016 qu'il y a un changement de point de vue vis-à-vis des hackers

RENS cyber ? Pour lui, souvenir armée au 13eRDP en soutien tactique.

Plusieurs types d'hackers éthiques selon lui : pentester, travail avec le gouvernement.

Il est en lien depuis qq temps avec le COMCYBER (probablement partenariat bientôt), notamment Yohan Bauzil, correspondant (CDT) COMCYBER en Occitanie/Toulouse. YB est aussi RSSI chez OneWeb Satellites (boîte US a priori), ss-traitant d'Airbus)

Il se dit « très patriote » mais pas naïvement, et dit se consacrer à des activités légales, a des convictions.

Mission pour Guardea (projet militaire), boîte de Marseille : missionné pour mettre en place (avec équipe) un système de surveillance, dispositif technique (surveillance sur mots-clés) sur SI de l'entreprise (**ou pour d'autres entreprises ?)**

OSINT ? Investigation numérique. **Pas plus. L'interroger plus tard davantage.**

En 2019, il s'est fait tamponner (DGSE ? COMCYBER ? → contact de ce dernier peu après – Yohan Bauzil, intéressé pour le recruter après entretien), DGSI ? →possible, il parle de la Cellule Richelieu, a priori cellule spéciale (de la DGSI ?) de hackers gouvernementaux, sous couverture.

Me donne des contacts VIP :

- Tris Acatrinei (profil juridique, assez médiatique), a créé le projet Arcadie (lien avec parlementaires)
- « Elie » : un ami à lui, en lien avec la cybercrim de Tlse aussi. Mission contractuelle pentesting pour un grand compte : anecdote : il aurait trouvé des failles non détectées par un ss-traitant cybersécurité du grand compte ! Aurait été un peu malmené à cause de ça. Et le grand compte se retournant contre son ss-traitant cybersécurité.

Bastien Ory (ami Séb) pourrait le connaître (ainsi qu'Alexandre Oda)

Il évoque lien avec Police (pôle cybercriminalité) à Tlse (Bld Embouchure), qui parfois fait appel à des détectives privés et, au-delà, des hackers. Lui a été qq fois sollicité pour les seconder. Mais se refuse à certaines de leurs demandes (réputation et par principe) parfois borderline.

Fait d'armes entre autres d'AOda : a hacké la MAAF (en full disclosure, ancienne pratique/protocole sans contrat de hacking, avant l'institutionnalisation des Bug Bounty). La MAAF lui a envoyé la police, bien qu'il les ait informés (un peu style Rabbin des Bois avec SciencePo. A ce propos AOda me dit qu'il s'est créé une image, mais qu'il peut être considéré comme hacker + ou -) D'ailleurs AOda me dit qu'il fait pareil et qu'il cultive volontairement cette image : il s'habille tjrs en noir par ex, en public…)

Il me parle de la pratique du confessionnal, consistant dans le cadre de grand-messes de hackers type « Black Hat », à divulguer (juste à cet auditoire) « Voilà, j'ai piraté un tel » → divulgation anonyme avec preuves (PoC)

Pour lui, d'accord avec l'idée du hacker comme agent de RENS.

Selon lui, les SR recrutent des Black Hats aussi [s'ils le peuvent ?! Parce que par principe, le voudraient-ils… ?].

Evoque qu'il ne veut plus former (sauf faire des meet'up plus tard), peut-être en bonne partie parce qu'un de ses anciens « apprenti » a viré de bord en le lâchant et lui disant clairement qu'il allait passer du « côté obscur ». Son pseudo : « cre$us »

Prend des stagiaires toutefois (est-ce que c'est possible en autoentrepreneur ?!)

Entre hackers, cooptation, P2P. → se font « baptiser ».

AOda : « Petit monde qui commence à sortir de l'ombre. »

Il connaît ***xorz***, un hacker français notoire (site web et compte Twitter), ***Micode*** (chaine Youtube).

Il s'amuse à pirater les pirates (et les **Red Rooms** qu'il ont créées sur le Dark Web), et il s'adresse à la Police (cybercrim Tlse) pour les dénoncer (désignation, URL…).

Ex (il n'y a pas contribué) de succès : la fermeture de frenchdeepweb.

Il est webmaster (ou modo) sur hackademics.fr (et m'invite à m'y faire connaitre de sa part (en le notifiant @maitreoda) pour prendre contact avec le petit monde)

Me dit que la coopération Etat-entreprise-hacker commence à émerger.

Les SR recrutent des Black Hats aussi (s'ils le peuvent ?! Parce que par principe, le voudraient-ils… ?).

Selon lui, ces liens sont ponctuels, utilitaristes, opportunistes. Il n'y aurait donc pas co-construction, de relation en réseau, de réflexion et de pratiques symbiotiques. De même avec les entreprises.

Très vite, les hackers éthiques se mettent en freelance pour juste de la coopération avec les SR, les entreprises, d'autres organismes de l'Etat. L'Etat et les entreprises ne coconstruisent pas avec les hackers, il n'y a pas de mise en réseau véritable. Et de leur côté, les hackers préfèrent également s'en tenir à ça (d'où leur indépendance), ils préfèrent s'en tenir là car ils ont assez de travail et ne manquent pas d'opportunités dans le contexte de la montée du risque cyber.

Evoque qu'il ne veut plus former (sauf faire des meet'up plus tard), peut-être en bonne partie parce qu'un de ses anciens « apprenti » a viré de bord en le lâchant et lui disant clairement qu'il allait passer du « côté obscur ». Son pseudo : « cre$us »

Prend des stagiaires toutefois (est-ce que c'est possible en autoentrepreneur ?!)

Entre hackers, cooptation, P2P. à se font « baptiser ».

AOda : « Petit monde qui commence à sortir de l'ombre. »

Il connaît x0rg, un hacker français notoire (site web et compte Twitter) [n'est-ce pas x0rz ?), Micode (chaine Youtube).

Il s'amuse à pirater les pirates (et les Red Rooms qu'il ont créées sur le Dark Web), et il s'adresse à la Police (cybercrim Tlse) pour les dénoncer (désignation, URL…).

Ex (il n'y a pas contribué) de succès : la fermeture de frenchdeepweb.

Pour lui, les spécialistes OSINT sont à part et ne sont pas à proprement parler des hackers, même si leur activité s'inscrit dans le hacking. En effet, ils font de la reconnaissance passive (me dit-il), donc il font du hacking dans une certaine mesure (c'est la première phase d'un hack, le footprinting, la prise d'info, la reconnaissance, le scaning). Et ça sert pour la cybersécurité où on en fait un minimum [d'autant plus dans la Threat Intel] pour tester les sécurité web et réseau.

Il évoque le Google Dorking, et dit que les BdD comme GoogleDork database, ça peut être « violent ». Dans le sens où on peut faire la chasse aux vulnérabilités Web.

L'investigation numérique, les assurances en font beaucoup, par exemple.

Pour lui, la psychologie humaine et la rétro-ingénierie sont les deux domaines, des particularités, les plus puissants et valorisants pour un hacker éthique (il évoque Baptiste Robert de Toulouse, sans le connaître personnellement). Ca donne de la lumière aux hackers (K. Mitnick, d'ailleurs, est présenté d'abord comme un fin « psychologue ». Donc l'ingénierie sociale (le HUMINT). Dit que le CYBER-HUMINT, c'est effectivement de l'ingénierie sociale.

Il évoque les méthodes par exemple policières concernant l'ingénierie sociale.

La méthode « de l'escalier » : méthode de réconfort , on joue sur l'émotionnel tout en manipulant pour faire se compromettre (dans ses dires notamment) les prévenus. Ca ressemble à la méthode d'interrogatoire du nazi Hanns Scharff.

On parle de VAULT, un outil-système dans le devSecOps, open source, qui est associé au « secret management ».

Le principe de VAULT est notamment de cloisonner les données et assets en les séparant pour moins les exposer globalement (ID d'un côté, mots de passe sur un autre serveur, etc.)

Il est webmaster (ou modo) sur hackademics.fr (et m'invite à m'y faire connaitre de sa part (en le notifiant @maitreoda) pour prendre contact avec le petit monde).

Hackademics a aussi un serveur Discord, plus simple pour le contacter.

« *J'ai été approché par des entreprises gouvernementales, le COMCYBER, par l'ONU et par les renseignements* [...]. *Ils m'ont accosté dans la rue c'était assez bizarre* [...], *ils m'ont dit qu'ils savaient qui j'étais et ce que je faisais et il m'ont donné une carte de la DGSE avec un numéro dessus.* »

*« Entre 2015 et 2017, il y a eu une grande vague de recrutement des hackers dans le monde par la Russie* [...]. *Ils repéraient des personnes actives et compétentes sur des forums pour leur proposer du travail* [...]. *Moi, à ce moment-là, j'ai vu des hackers français très bons partir en Russie ».*

« *Nous la France on est très silencieux, on fait pas beaucoup de bruit mais on est pas les derniers crois-moi* ».
Des organes comme la cellule Richelieu, une cellule de renseignement française où l'on trouve des hackers, ont été mis en place pour résister aux cyberattaques. Alexandre Oda donne de son temps pour aider la police et les autorités.

« *Je mène des actions pour trouver des grey et des black hats, je donne tout aux autorités et ils font leur travail* [...]. *J'aide les entreprises mais je vais aussi chercher les méchants au fond de leur trou, parce qu'il faut aller chercher le mal à la base* [...]. *Pirater c'est interdit, mais derrière tu donnes des accès à des groupes, tu fais avancer des affaires d'Interpol, tu leurs donnes des éléments supplémentaires…* »

« *En 2017 j'ai commencé à dire aux gens, vous allez voir, aujourd'hui les gens n'en ont rien à cirer, on nous prend pour des rigolos, des geeks, mais demain les entreprises vont courir pour venir nous recruter* ». Il dit que ce qu'il avait prédit se concrétise : le cyberespace prend désormais une place prépondérante, entreprises comme Etats ont compris la nécessité d'embaucher des gens performants pour assurer leur cybersécurité.

Entretien 17

| | |
|---|---|
| **Nom** | **HERTZOG Thomas** |
| **Date** | 14/06/2021 |
| **Fonction** | Pentester chez SecuLabs SA (Suisse) |
| **Expertise** | **Jeune hacker éthique/pentester/OSINT** |

Il est assez jeune (21 ans) donc pas trop d'expériences et de point de vue sur les questions politiques, etc. hormis le côté technique de l'informatique qui est ce qui l'intéresse vraiment.

Bénévole sur GitHub (il a déposé son outil Python d'OSINT sur Gmail, baptisé GHunt) et Hackthebox.

Il a été contacté (mais sans tamponnage) par un N-Tech ou plus exactement le chef du groupe de la lutte contre le cybercrime de l'antenne de la PJGN de Nice, via LinkedIn pour le féliciter pour GHunt en gros). Il n'y a pas/ne lui a pas répondu. Son apport chez Github avec son script GHunt lui a attiré un certain intérêt sinon il n'a pas été approché.

Il ne fait pas la différence entre renseignement cyber et OSINT.

Selon lui, l'Etat français organise de plus en plus de CTF. Il manifeste de plus en plus d'intérêt, mais T. Hertzog ne sait pas quels sont les liens réels entre hackers et Etat.

Participera à la conférence BARBHACK à Hyères, près de Toulon cet été 2021 (28 août).

https://www.barbhack.fr/en/

Entretien 18

| | |
|---|---|
| **Nom** | **BAUZIL Yohann** |
| **Date** | 06/09/2021 |
| **Fonction** | Ingénieur informatique, chez Airbus Oneweb Satellites (SAS), Correspondant zonal de réserve de cyberdéfense adjoint (CZRA) - ZDS Sud au COMCYBER. |
| **Expertise** | **Cybersécurité (RSSI), ingénieur réseaux/systèmes** |

Il passe par l'école 3IL (Limoges)

Ingénieur réseau/sys/sécurité

Il travaille ensuite chez Airbus DS et coordonne aujourd'hui l'IT (serveurs et réseaux) sur tous les sites d'envoi de satellites Airbus, puis RSSI chez via Oneweb, une coentreprise entre Airbus et Oneweb (anciennement société US et maintenant anglo-indienne).

Pour lui, le « cyber » est un terme galvaudé (marketé), il parle de RSI.

Le RENS cyber est plus large que l'OSINT.

COMCYBER

Militaire

Composantes : CALID (LIO) et CASSI (LID)

Il pense que le COMCYBER travaille de manière formelle avec les hackers.

En revanche le recrutement est plutôt tourné vers l'offensif (hackers éthiques/experts cybersécurité). Ils embauchement sur fiche de poste plutôt que sur profils (alors que les hackers disent tous que c'est par la pratique et les PoC qu'on prouve sa compétence).

Pour les relations informelles avec les hackers, c'est la DGSE et la DGSI, qui vont recruter des hackers blancs, patriotes.

« C'est en dessous des radars. »

Selon lui, dans l'ordre de priorité : d'abord, la DGSE, DGSI, COMCYBER.

Il a postulé au COMCYBER, il a repris le poste dévolu avant à Amaury de Gayardon (Airbus), comme correspondant régional du COMCYBER.

Politique de décentralisation // ZDSSud.

Rôle de correspondant : relais de l'état-major du COMCYBER.

Missions :

- Recrutement
- Rayonnement (RCO par ex. Rencontre cyber Occitanie)
- Veille techno
- CTF (proposition)
- Support local pour réserviste opérationnel.

Entretien 19

| | |
|---|---|
| **Nom** | **CURTET Florent** |
| **Date** | 30/09/2021 |
| **Fonction** | Hacker éthique, expert cybersécurité/pentester à son compte |
| **Expertise** | **Hacking éthique, ancien black hat** |

Sur son profil LI, il dit faire du renseignement offensif.

Très engagé, patriote, malgré son passé de black hat (arrêté par la police PJ de Nice, Pierre Pénalba, actuel chef de groupe de lutte contre la cybercriminalité à Nice (MININT).

Recruté par le COMCYBER via Yohann Bauzil.

RENS cyber : le renseignement, ça dépend de l'entité, personne, Etat, entreprise.

C'est du marketing. « Intelligence », « CTI » : en fait, c'est la recherche de menaces à venir ou existantes (menaces technico-informatiques)

On évoque l'OSINT. Il parle des Dorks, « *très puissants* ».

Le hacking est-il du renseignement ?

« *Oui, évidemment* ». C'est de la « recon » (acquisition passive d'informations) donc en grande partie de l'OSINT, à quoi on ajoute l'offensif (énumérer, casser les sécurités)

**OFF ---- Finalement, le livre de FC le révèle.**

Pierre Pénalba l'avait arrêté (Florent Curtet était black hat à l'époque donc). Devenus amis, il l'avait remis dans le droit chemin.

**------**

On l'a ensuite rappelé et donc il l'a mis en relation avec Yohann qui l'a contacté via LinkedIn.

Il a aidé l'Etat sur les questions de terrorisme, comme « honorable correspondant » (il le qualifie ainsi) de la DGSI.

Il a travaillé aussi pour l'AIEA à un moment.

Selon lui, DGSI et DGSE ont du mal à coopérer.

En ligne, il a trouvé beaucoup de données personnelles des membres du gouvernement Macron, qu'il a contactés à ce propos. Il a notamment appelé Gérald Darmanin, voyant qu'on ne lui répondait même pas. De là, le gouvernement s'est ravisé.

**Quelles relations entretient-il avec l'Etat français ?**

Ils passent par mails chiffrés ou Signal. (DGSI : uniquement Signal, sauf en cas de grosses données : il rencontre physiquement deux « agents », et échangent pas NAS ou disques durs. Il a des canaux/lignes d'urgence avec la DGSI)

Il leur donne beaucoup de signalements (alertes).

Il donne des axes. Et signale des données qui circulent/stockées (Dark Web notamment)

Il a eu affaire avec les Etats-Unis à un moment donné (qui le prenait pour un agitateur pro-russe, ou un crypto-partisan de la Russie, « un ingérant russe »). Il a eu accès à des données qui l'ont fait être contacté par le DoD US (il a bénéficié d'une protection policière française). Il utilisait avec le DoD une application de communication (sorte de Discord chiffré) appelée MATRIX.

**PAS DE COCONSTRUCTION AVEC l'ETAT. Ça reste du ponctuel/utilitariste. Il fait beaucoup de chose en bénévole (comme son intermédiation criminels/entreprises).**

Il évoque les multiples enquêtes de sécurité sur lui par la DGSI, on a testé sa fiabilité, et ensuite *« on te débloque des facilités financières et techniques. Mais pas d'infos sur les interventions a posteriori des signalements* ». Il dit qu'il est « *une donneuse* ».

Pas de projets communs, chacun reste dans sa sphère.

Avec l'ANSSI, pas de souci de communication (moins opaque), le canal est ouvert et il est souvent en contact avec eux. Mais ils ne donnent toutefois pas beaucoup d'infos.

**OFF ------**

Pour lui, l'ANSSI : « ils se prennent pour un service de renseignement ! Mais ce ne sont pas des hackers, et ils se prennent pour ce qu'ils ne sont pas. »

**-------**

Et d'ajouter qu'ils sont faciles à contacter mais hermétiques dans les échanges.

On lui fait comprendre en off (certains membres de l'ANSSI) que « *c'est super ce que tu fais, mais tu comprends, à l'ANSSI, on ne comprend pas trop que tu en saches plus que les autres*. »

Il parle de jalousie. Il invoque la « *frilosité de l'Etat* ». Esprit « *bastion* », « *quasi-sectaire* ». « *Fausse politique du secret* ».

Il parle de Guillaume Poupard, son directeur (2014-2022). Il est de bonne constitution, mais « *il applique des dogmes.* »

Selon lui, « les USA sont bien plus matures sur la question de l'intégration entre hackers et autorités publiques. Il y a un gros problème de communication. »

Même dans le recrutement, la différence est notable // USA (la NSA passe par exemple pour sa dernière campagne de recrutement par des jeux de pistes avec de la stéganographie, etc. – déjà un premier filtre pour juger la compétence des candidats).

**Quelles relations entretient-il avec les entreprises françaises ?**

Exemple de relations avec une entreprise (grande) : Réponse à incident : un de leurs clients a été piraté. Florent Curtet peut-il faire du renseignement sur le Dark Web pour voir si ses données ont été diffusées ?

Il dit qu'il a décidé de jouer franc jeu quant à son passé de *black hat*, le révélant à ses clients privés. Ça refroidit certaines, d'autres non.

Il a fait ses armes dans des cabinets de conseil (quelle nationalité ?!), puis a monté son entreprise individuelle (NéoCyber) au cours de la crise sanitaire.

Il avait fait une école de commerce après avoir été appréhendé lors de ses activités illégales. Mais son expérience d'enseignement supérieur ne l'a pas du tout convaincu. Donc il a décidé de revenir très vite à sa passion (contact avec autorités…)

En tant que bénévole, il joue les intermédiaires avec certains groupes cybercriminels (comme Everest), souvent est-européens. Il fait le relais et a un rôle d'intermédiation et de temporisation dit-il. Entre la France (autorités) et certains groupes cybercriminels. Il parvient à les convaincre de « limiter la casse » pour les victimes. Avant, ils auraient diffusé tout sur le Dark Web et auraient bloqué les entreprises (avec impact fort, jusqu'à liquidation). Désormais, il empêche ou minimise des leaks car il réussit à se faire respecter d'eux, et ils le consultent d'abord. Ainsi, cela va minimiser l'impact sur les entreprises victimes, qui ne seront pas bloquées, ou qui auront le temps de se retourner.

Il joue donc un double jeu : les sociétés ont le temps de faire une sauvegarde…

Il a déjà fait de l'ingénierie sociale avec des clients privés (se faisant passer pour un salarié d'entreprise (par exemple à cause de qui – mauvaise hygiène informatique, mots de passe faibles – la société a été attaquée) et face à des cybercriminels (forçant la victimisation pour rendre plus empathique ces derniers).

Il dit que ces cybercriminels de l'Europe de l'Est ne sont pas tout noir, et qu'ils sont avant tout pauvres.

« Ils ont un peu d'éthique, dans leur connerie ».

Il m'oriente vers Julien Dugay (expert CTI pour Capgemini Toulouse).

Entretien 20

| | |
|---|---|
| **Nom** | **LEGAY Julien** |
| **Date** | 13/10/2021 |
| **Fonction** | Expert Threat Intelligence chez Sogéti. Ancien chercheur en physique et autodidacte en hacking. |
| **Expertise** | **Hacking, CTI** |

Ancien chercheur en physique et autodidacte en hacking.

Premier moteur : intégrer le monde académique dans le Sud, et après opportuniste par un ami qui s'était reconverti lui aussi et qui l'a appelé à venir chez Capgemini.

**CTI ?**

Définie par les intérêts de l'entreprise (ici Capgemini) ESSEC.

CERT – missions : anticipation, détection, réponse aux accidents. Ça a démarré en 2015 mais bcp de contraintes. Un ancien de l'ANSSI qui est venu structurer ça pour avoir la forme d'un CERT. Ils avaient déjà un SoC. Un peu un prolongement avec l'Etat. Les CERT régionaux.

La CTI : construire de la connaissance sur le paysage de la menace : capitaliser, créer du rens (niveaux tactique, stratégique, et opé.

**Renseignement cyber, la CTI**

Ça vient du monde anglosaxon et militaire.

Cycle du rens, appellation, techniques et méthodes, PsyOps…

Opportunisme marketing autour de la CTI. Pyramide de la douleur, il connait.

Travaille sur IoC beaucoup. Etude des TTPs (MITRE ATTACK – grosse bibliothèque/encyclopédique de signatures d'attaques/TPPs, étatique US à la base, mais mature aujourd'hui). Téléchargeable, permet de trouver des infos sur les TTPs utilisées – création heatmap.) Chez Capgemini, ils en ont une aussi biblio de signatures.

Impression qu'il a : a changé son fusil d'épaule dans l'offensif. DU moins dans l'éducation. La France a été plus frileuse. Bcp d'acteurs étatiques vont dans le privé (son chef est un ancien DGSE). Mais officiellement, hackback ou hacking offensif ça sera la DGSE ou du militaire et c'est classifié. Méconnaissance de la partie judiciaire dans le hacking et l'offensif. Donc on est frileux en France. Est-ce qu'on interfère avec une opé en cours de la part de l'Etat. Plein de gens pourrait faire le l'offensif, mais rien n'est cadré dans cet aspect de l'offensif. Les clients économiques n'abordent pas trop l'offensif.

L'ANSSI est très fileuse et à cheval sur le juridique, moins les anciens de la DGSE (son supérieur).

L'ANSSI a plus d'influence sur les acteurs économiques (dont Capgemini), donc on reste dans cette logique de frilosité et de rapport au droit.

**OSINT :** sur réseau anonymisé ou pas. Ils en font et face aux criminels de ransomware. Donc pas mal de recherche et recoupement d'infos sur les TTPs et rarement sur les acteurs attaquants. L'attribution est très délicate (quand c'est seulement possible) mais pour les entreprises, c'est encore plus chaud parce que ça devient de la politique.

Entretien 21

| | |
|---|---|
| **Nom** | **« Bob » (anonymisé)** |
| **Date** | 15/10/2021 |
| **Fonction** | Chercheur en cybersécurité à l'ANSSI, hacker/OSINTer. |
| **Expertise** | **Hacking/OSINT/cybersécurité** |

Travaille à l'ANSSI (sous-direction opération) depuis 2019 et est passé par le privé (cabinet de conseil SSI, 11 ans d'expérience).

Pour lui, être hacker est un vrai métier.

La NSA (unité TAO (Tailored Access Operations), sorte de RIC/CTI (équipe qui identifie, surveille, infiltre et recueille des renseignements sur les systèmes informatiques utilisés par des entités étrangères aux États-Unis.) Une vraie équipe de hackers-fonctionnaires selon x0rz, anciens informaticiens experts en cybersécurité qui font de l'offensif. [Sorte de hackers-corsaires]

Des agents de la CIA, via du HUMINT, recrutent des hackers pour des actions offensives, dans une logique de recrutement de mercenaires.

Offres d'emploi d'agences françaises sont passées sur LinkedIn (en lisant entre les lignes, on le voit).

Besoin utilitariste en France concernant les hackers.

Le cadre légal existant est très prégnant.

Challenges ouverts par la DGSE pour le recrutement ou du moins la possibilité de faire émerger des jeunes notamment, précoces dans leurs capacités en informatique.

Il y a le problème de l'habilitation secret défense liée à ces métiers.

Est-ce qu'il y a une voie pour le recrutement de hackers (au-delà des informaticiens en sécurité informatique), au sens propre, avec l'approche alternative, iconoclaste qui les caractérise ?

Il y a un curseur, un juste milieu (même si les profils classiques sont privilégiés). Il corrobore pour Viginum. Pas sûr que ce soit très efficace, et dont l'objectif n'est pas très clair.

Chine, acteur extrêmement offensif.

Aspect culturel important dans l'approche en France : on ne trouve pas la cohésion d'un Etat-nation comme Israël, où tout le monde se connait (et toutes les grandes étapes de socialisation qu'on y trouve, ses liens société civile-armée).

Pas dans la culture française (syndrome barbouzerie), méfiance pour le recrutement et aussi les questions de rémunérations (limitée, fonction publique).

Le cyber renseignement : l'OSINT en fait partie + méthodes (d'espionnage) de collecte de renseignement à travers le cyber (actions offensives)

ANSSI : il y a des auditeurs pentesters.

« On ne va pas recruter le mec « autiste-mais-génie-dans-son-coin ».

« On n'est pas assez nombreux, il faudrait être dix fois plus face à la menace. »

L'ANSSI peut être vue un peu comme du contre-espionnage, en vertu du flou qui entoure désormais l'ère du numérique.

**Liens hackers-entreprises**

Niveau faible en moyenne des salariés dans les entreprises. Les « bonnes pratiques » passent en premier et sont plus ou moins bien suivies. Ce qui est déjà pas mal, mais concerne les plus grandes ou certaines plus petites. Dans celles-ci, des hackers ne sont pas très utiles.

En revanche, ils le sont vraiment pour les grandes entreprises.

Pourquoi tant de vulnérabilités informatiques ?

Il y a une « dette publique » à cause de la facilité en termes de programmation.

Beaucoup de code est repris, par exemple Windows 10 ou 11 contient beaucoup de morceaux de code des anciennes versions.

En tant que membre de l'ANSSI, il avoue pourtant que concernant le SecNumCloud, certification de sécurité accordée aux clouds étrangers (américains) : « on met du scotch ; c'est de la rétention minimale de données. »

Difficile d'être souverain selon lui, et notamment parce qu'il n'y a aucune vision stratégique de la part du gouvernement, à part une vision court-termiste. Il parle de « bullshit de la start-up nation de Cédric O. » On occulte un peu trop la réalité dans la culture de la communication politique.

Entretien 22

| | |
|---|---|
| **Nom** | **POUCHERET Victor-Louis ("doomer")** |
| **Date** | 14/11/2021 |
| **Fonction** | CTO BZhunt, hacker éthique |
| **Expertise** | **Hacking éthique/cybersécurité** |

En tant que citoyen, il n'y a longtemps pas eu de moyens pour faire remonter les vulnérabilités informatiques.

Grâce à la « loi de 2016 (article 47-L23…) pour une République numérique », c'est désormais possible et ouvre donc la voie au hacking éthique, au bug bounty…

C'est une première valorisation du hacking que l'on doit aux prédécesseurs, la génération précédente des hackers, de la « communauté » (les Yogosha et consorts).

**La communauté (ou les communautés) du hacking :**

Passion de la cyber, donc job dédié, profil cybersécurité mais orientée offensive (Red Team, bug bounty…)

La communauté est faite de savoir-faire très spécifiques (par exemple, spécialité malware sur smartphones, 0day, rétroingénierie…)

Plusieurs communautés sans doute : en fonction des compétences classiques type SSI/cybersécurité, l'offensive et les « vrais » hackers, la « bidouille » technique/physique avec un profil comme Damien Cauquil…

Il y a aussi une certaine démarcation entre les spécialistes défense et ceux de l'offensif. Monde assez différent, mais qui devrait faire greffe pour une meilleur cohésion (et vis-à-vis notamment d'une dynamique patriotique).

Ces communautés sont visibles sur les RSN (Discord et les plus classiques, Twitter, LinkedIn) : beaucoup de discussions et on reste sur les pseudos par exemple.

Monde assez petit. On se connait tous plus ou moins, de près ou de loin.

Lui, V-L Poucheret, ne travaille pas pour l'Etat, mais son expertise peut être appelée via des appels d'offres au profit d'entités paraétatiques ou totalement privées, avec des niveaux de confidentialité le cas échéant.

En France, on est loin du cliché du cinéma du hacker qui va faire de l'offensive.

Toutefois, certaines entreprises, comme Diateam (diateam.net) proposent leurs propres solutions auprès des ministères pour la cyberguerre. [Et même si elles se présentent plus conformément à l'éthique en France comme proposant des solutions de la cybersécurité (avec Red Team…)]

Implication partielle avec l'Etat vis-à-vis de la cyberguerre.

Selon lui, l'Etat français peut possiblement acheter de la 0day.

L'exemple du logiciel d'espionnage Babar (conçu par la DT de la DGSE, ce qui a été confirmé officiellement par son ancien DT, Bernard Barbier) dont la fuite provient des papiers Snowden.

Il y a un retard et une non adéquation entre les problématiques et le contexte actuels par rapport au fonctionnement administratif d'une manière générale en France.

Le cadre juridique pose le problème de l'adaptation avec la communauté du hacking (il parle de plusieurs communautés en réalité de hackers, peut-être parce que c'est de l'éthique, et que la cybersécurité plus classique n'est jamais loin).

Quelques exemples de tentatives : le DG'hAck (CTF de la DGA) [la DGSE avec le CTF challengecybersec en direction du grand public (à des fins de recrutement) ou des jeunes de lycée avec Alkindi]

Ce genre d'initiatives avec les éléments évoqués plus haut montre qu'on est sur la bonne direction en France. Mais il y a une question d'upscaling à faire. Et notamment, faire face à « la lourdeur administrative incroyable » ne serait-ce que vis-à-vis des appels d'offres publics. Ce n'est évidemment pas agile.

Les programmes de Bug bounty pour le compte des entités de l'Etat montre une vraie implication des hackers.

Par exemple, pour « la mise sur le marché » de l'application StopCovid avec Yeswehack, ou le MAE ou le MININT (ANEF : Administration Numérique des Etrangers en France.). On n'est pas encore à une implication en amont des projets, mais quand même au milieu et en aval du processus sécuritaire.

Donc appel à la communauté du hacking française.

**Hackers // entreprises**

Les rapports dépendent du niveau de sensibilisation, et donc du degré de maturité, qui a crû depuis les grandes cyberattaques de 2017 et la crise du Covid avec le télétravail accru.

Donc les entreprises cherchent de l'expertise sur l'offensive.

En revanche : on n'est pas dans une approche globale de la sécurité.

Courbe positive toutefois au niveau de la sensibilisation.

Un des problèmes actuels est la question de la qualité des sous-traitants et de leur niveau d'exigence. Les entreprises savent qu'il faut se mettre à la page concernant la sécurité informatique et numérique mais elles ne savent pas vraiment ce dont elles ont besoin car la matière est pointue, y compris pour des équipes d'informaticiens classiques (IT : Information technologies, l'IT n'est pas la SSI et encore moins la cybersécurité, mal comprises des dirigeants). Et beaucoup se font berner et subissent de forts tarifs parfois voire souvent injustifiés. Donc il y a une responsabilité éthique de la part des sous-traitants.

Qu'en est-il de l'internalisation de ces activités de sécurité ?

Elle est difficile à réaliser car il n'y a pas de savoir faire correct en interne, et compte tenu que les meilleurs spécialistes sont d'esprit indépendant. La position du hacker en général, c'est un peu l'image de l'électron libre. Et il faut un esprit d'attaquant, et dans l'actualisation perpétuelle des connaissances qu'il s'agisse des outils, des progrès de la technologie et de la cybermenace.

[Les hackers jouent de ce positionnement d'indépendant et sous-traitants car ils savent par ailleurs qu'il y a pénurie de profils]

Anecdote : les RSSI du CHU de Brest. Un an au poste et ils en ont déjà marre. Comme dans bien d'autres organisations, il y a un cruel manque de ressources allouées à la sécurité informatique.

Il y a une jonction, un équilibre à faire, dit V-L Poucheret, entre les ressources internalisées et la collaboration avec des « attaquants » externes. Il y a toutefois une certaine continuité à ce sujet dans certaines entreprises.

Quelle est la profondeur de la collaboration ?

BZhunt (son entreprise de consulting) accompagnent parfois sur du long-terme : 3/5/10 ans. Il y a une forte implication et une grande confidentialité [il ne peut évoquer l'identité de ses clients, mais il s'agit pour la plupart d'acteurs industriels, dans la mécanique comme la fabrication manufacturée, plutôt grandes entreprises qui externalisent ce qui requiert une forte expertise]. Il y a de l'occasionnel comme du plus impliqué.

Selon lui, il vaut mieux que les sous-traitants (hackers) gardent leur indépendance, mais faire avance les connaissances des salariés internes (informaticiens défense) pour faire progresser l'organisation selon son cycle de vie.

**Hacking = renseignement ?**

Oui, clairement. Le hacking est une pénétration dans la bulle du secret, grâce à l'agrégation d'informations.

L'OSINT est un sas d'entrée incontournable pour connaître les développeurs/webmasters/informaticiens et leur manière de penser, leur background, leurs patternsn les technologies utilisées (matérielles, logicielles-applicatives), leurs passifs (comptes leakés, documentation exploitable…), le floutage entre les activités/vies privées et publiques/professionnelles et personnelles.

La communauté OSINT est de bonne constitution.

Assimilation entre OSINT et hacking. Selon lui, l'OSINT c'est du hacking car il y a la même philosophie de la « bidouille », donc un « OSINTeur » est un hacker. Il y a le même état d'esprit de se dépasser ; de se remettre en question sur la perception d'une image, d'un phénomène ; et de remettre en question le fonctionnement d'une chose, d'une machine. [C'est de la « bidouille intellectuelle » ?] Oui, absolument dit-il. Pas au sens spécifiquement technique, bien qu'il y ait des OSINTeurs doués en informatique. Pour lui, ce n'est pas une discipline spécifique. Les hackeurs font d'ailleurs de l'OSINT, et le cycle du hacking comporte cette collecte dite passive d'informations.

L'ingénierie sociale et l'intrusion physique sont aussi très rattachés au hacking.

**Les hackers et l'Etat ne communique que peu**, c'est ponctuel sur une sujet précis, ou via les appels d'offres publics indirects.

Il y a la question des valeurs de la France dont le pays en général fait grand cas. « C'est ce qui fait partie de notre identité nationale. Et ça entrave peut-être notre progression en termes de cybersécurité. »

**IA et hacking/cybersécurité**

L'IA, c'est encore l'âge de pierre.

Même les réseaux neuronaux sont peu développés.

Côté offensif, il n'y a rien, et côté défense beaucoup de poudre aux yeux et de com'. Les applications actuelles sont balbutiantes.

**Qu'en est-il du Campus Cyber ?**

Seules des grosses entreprises pour l'instant en font partie.

Il y a d'autres initiatives comme France Cyber Maritime, association loi 1901.

**Le COMCYBER ?**

Pas de connaissances. Il fait des opérations offensives mais c'est placé sous le sceau du secret défense.

**L'ANSSI**

« Depuis l'arrivée de Guillaume Poupard, l'ANSSI a une belle plus-value ». Elle fournit beaucoup de données et de guides techniques.

**Souveraineté numérique française ?**

« C'est évidemment encore insuffisant. »

Entretien 23

| | |
|---|---|
| **Nom** | **DOMINGO Clément ("saxX")** |
| **Date** | 15/11/2021 |
| **Fonction** | Hacker éthique franco-sénagalais. |
| **Expertise** | **Hacking éthique/OSINT/cybersécurité** |

Dans la perspective étatique, officiellement, en France, on ne travaille pas directement avec les hackers. Officiellement, il n'y a pas de hackers.

Avec les entreprises, il existe des ingénieurs en cybersécurité (pentesting, Red Team).

Clément Domingo est, selon ses dires, l'un des pionniers du bug bounty, avec YesWeHack.

Cette activité du bug bounty a pu contribuer à officialiser l'activité du hacking/hunting (hacker/hunter).

Il y a plusieurs activités liées au bug bounty : rétroingénierie, test d'applications, pentesting…

Dès lors qu'un hacker travaille pour un service de renseignement (SR), un titre/poste est affecté à ce dernier en vue d'une mission. C'est donc très cadré juridiquement. Dès lors, s'il communiquait par exemple via les RSN, il disparaitra du champ, il ne communiquera plus publiquement ou ne participera plus à des CTF. On peut donc voir à quel moment tels profils sont passés au niveau d'un rapport contractuel et professionnel avec un SR.

Avant, on parlait cyberdéfense, maintenant on parle cybersécurité (LID, LIO).

Très peu parmi les meilleurs spécialistes du hacking travaillent en France (mauvaise valorisation à tous égards).

Les vrais hackers, selon lui, sont des autodidactes et n'ont pas de diplôme d'ingénieur en sécurité informatique.

**COMCYBER**

**Il est en rapport avec lui. Mais il tait la nature et la densité de ces rapports.**

Ils recrutent mais ils ont du mal à trouver des profils confirmés.

D'anciens de la DGSE montent leur affaire (exemple de TETHRIS dont la cofondatrice est l'une des pionnières à quitter le service dans ce sens). Ou alors ils vont travailler pour des entreprises du type GAMAM (ex-GAFAM) au moins quelques mois, « pas par manque de patriotisme, mais parce que ça s'y prête et qu'ils ont le « mindset » compatible (hacking/rétro-ingénierie, conférences…), ils sont ouverts d'esprit ». « Même les RH dans les entreprises classiques et notamment française n'ont pas le mindset. »

Difficile pour ceux-là d'aller ensuite vers le public/l'Etat.

Même la culture du travail décalé (encore faible en France // pays anglosaxons ou Allemagne où c'est plus développé et plus libre) est un frein indirect (administration française notamment, et même en entreprise, sauf sociétés spécialisées, spécifiques)

Anecdote : la ville de Rennes est une sorte d'incubateur où on est très actif dans la cybersécurité. [La Bretagne est connue pour héberger le PEC, Pôle d'excellence cyber.]

Mention et comparaison avec la NSA avec l'exemple du recrutement atypique/alternatif/officieux/moins cadré. Site web de la NSA : plateforme de recrutement via une sorte de CTF en soi (indices, cela requiert des compétences techniques pour trouver les « offres d'emploi ».) « A la NSA, il n'y a presque que des hackers, souvent des blacks hats qu'on a choppés. »

Certains Etats utilisent des simulations de cas, « un peu borderline ». Clément Domingo ne veut pas le nommer (pays anglosaxon) où on fait tester par des candidats les sécurités d'un site web par exemple, a priori anodin, mais il s'agit en réalité d'une attaque réelle contre un Etat étranger.

Avec G. Poupard de l'ANSSI, il y a une ouverture avec la communauté des hackers. Même Alain Juillet avait permis une certaine ouverture.

« Ça se démocratise. »

**COMCYBER**

L'organisme travaille avec des compagnies en son sein.

Il y a beaucoup à construire (attractivité, contenu).

C. Domingo travaille avec lui (mais souhaite rester évasif quant à leurs rapports // mission en cours)

Il a sans doute été contacté par la DGSE. A demi-mot, il dit « on ne sait pas qu'on va les rencontrer. » Il avoue en creux être ou avoir été en contact avec le service.

D'autres hackers flirtent eux avec la limite et donc la légalité.

**Le hacking : du renseignement ?**

Oui. Notamment, les phases de reconnaissance (active et passive – la moitié du travail selon lui) auprès des SI (« systèmes techniques et systèmes humains »).

Informations utiles et « intelligentes » (sic) sur les personnes (ingénierie sociale). Niveaux de profondeur de la cible…

Anecdote sur le rôle important de **Telegram**, l'application de messagerie instantanée chiffrée : une mine d'informations entre clear/deep/dark webs.

Lui-même s'est codé un bot (via une API) pour veiller sur Telegram et qui traduit à la volée des sources variées en langues étrangères. Il réalise donc une veille spéciale pour du « pattern matching ».

**OSINT**

L'OSINT n'est pour lui pas du hacking à proprement dit, mais c'est une composante du hacking et le hacking peut être une partie de l'OSINT.

**Campus Cyber**

Se cantonne à un projet immobilier plutôt qu'autre chose pour l'heure selon lui.

Une synergie avec les indépendants (hackers) ?

Selon lui, c'est pour l'instant beaucoup de com'.

**CTI (Threat Intelligence)**

RIC (renseignement d'intérêt cyber selon l'Etat ou des entreprises paraétatiques [comme Thalès], c'est de la CTI quoi qu'il en soit). Et ça concerne les entreprises proches de l'Etat, et concerne des enjeux étatiques, le niveau étatique (TTPs, attribution, IDs des cyberattaquants…).

« Ça rebondit sur la géopolitique. » Le cyber a une vraie répercussion.

Entretien 24

| | |
|---|---|
| **Nom** | **DOUZET Frédérique** |
| **Date** | 30/03/2022 |
| **Fonction** | Professeur des universités (Paris 8-IFG). |
| **Expertise** | **Géopolitique du cyberespace, approche théorique des questions cyber** |

**Notion de « communauté de hackers » :**

Les hackers sont ouverts d'esprit, faciles à appréhender.

La notion de communauté est vaste.

L'intérêt lucratif est important, mais les signalements responsables sont réalisés.

Ca reste ambigu avec par exemple un marché des vulnérabilités [0day, les Etats en sont parties prenantes aussi]

Il y a un encouragement du hacking dit éthique aujourd'hui (concours/bug bounty).

Recherche de profils atypiques autodidactes désormais.

**Son concours à a pensée cyberstratégique (membre du comité de la *Revue stratégique de défense et de sécurité nationale* en 2017-2018)**

Pas de préconisations sur l'emploi ou la contribution de hackers français.

**COMCBYER**

Recrutement dans la communauté amateurs avec l'esprit, le *mindset* « hacker ». On essaie d'attirer les profils (hackatons, concours…).
Aux USA, ça fait longtemps.

**RENS et OSINT**

FD fait la différence entre renseignement et l'OSINT, la recherche en sources ouvertes préfère-t-elle. Les chercheurs et les entreprises, on s'interdit de dire qu'on fait du renseignement. Et ce n'est selon elle pas la même chose.
Toute la société change, mais pas le renseignement (activités des SR d'Etat). Tout se numérise, les activités humaines laissent des traces numériques, des empreintes. Les conflits aussi laissent de telles traces. [métadonnées]
Donc, n'importe qui peut utiliser ces méthodologies et techniques pour collecter de l'information en sources ouvertes.

Et l'OSINT peut se révéler plus productif que le RENS d'Etat (plus de moyens et de ressources démultipliés). Bien sûr, le RENS (les SR) fait de l'OSINT. Mais les gens qui font de l'OSINT ne font pas de RENS.
Bouleversement du domaine du RENS : l'enjeu n'est pas l'accès à l'info mais le filtrage du bruit. Il faut produire et tirer du sens de ces mégadonnées.
C'est là que l'expertise en géopolitique [en fait plus globalement en sciences humaines, géoéconomie/IE…]. Cela permet de contextualiser (représentations géopolitiques).
Cela nécessite de plus en plus de profils hybrides.
Je lui parle de la CTI (threat intel), elle acquiesce : cela montre l'hybridation expertise technique + analyse géopo.

L'écosystème des entreprises avec leurs spécificités propres font de l'OSINT [OSINF ?]. Certaines sont spécialisées (en France : Preligens, Visibrain…) et proposent parfois des solutions de hackback. Celles qui font de l'offensif, en revanche, sont parties aux USA. Des entreprises fçaises peuvent développer de telles solutions offensives mais en droit, elles ne peuvent être en relation qu'avec l'Etat.
Les chercheurs aussi s'appuient sur les sources ouvertes. FD parle de l'IFG et de leur cyberstratégie challenge au FIC. L'IFG forme des apprentis qui ont vocation à travailler dans les SR.

**Campus Cyber**
Grâce à l'ANSSI : ouverture vers la recherche académique et privée.
Le projet peut nourrir la formation en cybersécurité en France.
Selon FD, cela a du sens en théorie, et constitue une bonne idée pour la collaboration (interactions par la proximité des bureaux). Elle ne connait toutefois pas les lieux.

Entretien 25

| | |
|---|---|
| **Nom** | **METAYER Julien "Kermit"** |
| **Date** | 30/03/2022 |
| **Fonction** | Consultant freelance hacker "éthique"/pentester (basé à Lyon). |
| **Expertise** | **Hacking "éthique", pentesting, cybersécurité offensive** |

**Liens avec entreprises**

JM travaille avec le privé (les entreprises). Il est pentester et formateur en sensibilisation pédagogique sur le phishing.
Les entreprises ne demandent pas aujourd'hui de diplômes ou de certifications en général. Elles s'en remettent au bouche à oreille et à l'efficacité de la prestation (après pratique et travail reconnus → recommandation des entreprises). Par exemple, en tant dévops, il a déjà un réseau de clients qui lui en amènent d'autres mais en pestesting. Surtout après attaque.
Le lien est froid, « glacial » selon ses mots, car les hackers sont soupçonnés d'être à la source du problème qu'ils identifient et font remonter. [rejoint les propos de F. Epelboin].
En tant que freelance, il est un conseil. Mais les plaintes sont évidemment établies auprès de la gendarmerie, qui passe l'affaire à des entreprises certifiées par l'ANSSI.
Mais il n'y a pas trop de législation (nationale, et internationale commune – supranationale donc) sur ce point et donc pas trop de certifications (sauf l'OSCP, qui est une certification privée américaine, assez reconnue mondialement et attestant légitimement de compétences, car l'examen est de très haut niveau).
Il n'y a d'ailleurs pas de cursus de formation universitaire/supérieure purement axée sur la cybersécurité [et encore moins l'offensif/le pentesting…]. C'est la plupart du temps des spécialisations dans un tronc commun (du type administrateur réseau/système – « sysadmin »). Tout est très tourné vers le défensif (même l'Ecole 42, l'Ecole 2600 (Yvelines)) [une école très récente vient d'apparaître aussi, et il y a des licences spécialisées « hacking éthique » - à Valenciennes].

Un 3e type de lien peut exister avec les entreprises concernant la sollicitation contractuelle : la sous-traitance auprès de cabinets de conseil (Deloitte, etc.)

Evocation des sources d'infos pour les hackers (en rapport avec les vulnérabilités/leaks de données) : raidforum (fermé récemment par le FBI a priori, mais revenu), des forums Telegram.

**Entre Etat et entreprises : le campus cyber**

Son avis : pas sûr que ça fonctionnera bien, à cause des liens contractuels liant chaque acteur avec ses propres clients.
JM est partisan de décentraliser plutôt.
C'est en partie le cas, avec le PEC à Rennes…

**Liens avec l'Etat**

L'Etat ne fait pas appel à lui et à son type d'entreprise individuelle [or, plusieurs autres hackers sont approchés individuellement par les autorités/les SR/la police].
Selon JM, l'Etat – à travers l'ANSSI – cherche des experts certifiés. Souvent pour la gestion post-incident (forensic) et en défensif (cybersécurité).
La cybersécurité offensive n'est pas très développée en France. L'Etat n'utilise pas des pentesters freelance.

Le « réservisme » permet déjà d'établir une passerelle.
Avant, on recrutait sur « faute » (DST) les hackers amateurs.
C'étaient des « correspondants ».
Aujourd'hui, selon JM, c'est surtout par l'intermédiaire de l'armée, et pas vraiment des civils.

Il a néanmoins un contact et travaille avec l'Institution de gestion sociale des armées (IGESA) relevant du MINARM.
L'IGESA ne fait pas appel à l'expertise cyber par elle-même, donc elle sous-traite via des entreprises dotées d'une certification à renouveler auprès de l'ANSSI.

**Le hacking/la cybercriminalité**

Le principe central, en droit, est l'intention. C'est ce qui va caractériser les activités en légales ou illégales. D'où la contractualisation de l'activité des hackers dits « blancs » avec les entreprises.
Il y a un manque généralisé de spécialistes en cybersécurité, dans l'Etat aussi. Et une concurrence entre l'Etat et les entreprises à cet égard, car ces dernières paient bien mieux les hackers.

Les entreprises sont aussi plus proactives.

Les hackers/pentesters ont une vision (le mindset) et chacun leur approche ; et les entreprises font appel à plusieurs profils sur plusieurs années (pour rater le moins de failles possible).
Il peut y avoir une fidélisation sur le long terme [sic] (2/3 ans), mais pas sur le très long terme.

Si incident après pentest → rappel pour régler le problème, et donc faire plus du défensif.

**Qu'en est-il d'entreprises spécialisées comme TEHTRIS en France ?**

Selon JM, culture du secret autour de la cybersécurité [TEHTRIS ne répond pas à mes sollicitations du reste].

Lui [comme d'autres hackers] a pris le parti d'être communiquant.

Selon lui, il n'y a pas de partage de savoir-faire entre hackers dits éthiques [rejoint F. Epelboin], contrairement à ce qui se passe entre hackers noirs (cybercriminels).

Aux USA, il y a beaucoup de clubs de hackers (avec un esprit collaboratif) qu'on n'a pas en France [rejoint totalement F. Epelboin]

Il y a un début de rapprochement (mais ça reste pour l'instant une coquille, et c'est à but politique/militant) avec « Hackers sans frontières », monté avec F. Curtet, C. Domingo…

Ce cadre comme les CTF (donc les concours de hack) leur permettent de se rencontrer en vrai (souvent on retrouve les entreprises-clés comme Sogeti, Capgemini…). C'est là qu'ils apprennent à se connaître. Mais sans échange de pratiques et sans projet concret collectif.

Il y a une séparation vie publique/privée.

Et il y a une « grosse défiance » vis-à-vis du statut autoproclamé de « hacker ». Il y a un côté « chacun pour soi ».

**L'OSINT**

Réglementation. Ce qui est possible aux USA ne l'est pas en France par exemple. Il faut chez nous une licence de détective en fonction des enquêtes traditionnelles.

Mais flou juridique sur l'OSINT en informatique. Encore une fois, on s'en réfère à l'intention.

Les SR :

Difficile de savoir de quels outils ils disposent, quelles bases de données.

Aleph-Network (entreprise française) travaille avec le MININT. Est-ce pour autant encadré (notamment vu les produits et l'activité spécifiques d'Aleph-Network, dans le dark web | crawling du dark web VS cybercriminalité) ? [derniers textes de loi montrent que le secret défense/les question de sécurité nationale peuvent permettre certains agissements non règlementés].

Selon JM, il y a des liens de confiance, ce genre d'entreprises est en cheville avec l'Etat, pour que les autorités puissent intervenir, ici pleinement dans le cadre du droit.

Le cadre juridique est plus ou moins rigide selon la thématique. Des fois, il faut passer outre.

JM évoque le cas d'absence de lien entre autorités et hackers comme lui, lorsqu'il s'agit d'affaires de cyber-harcèlement [/ doxxing] : les autorités ne donnent pas suite à ce que peuvent apporter (preuves numériques, témoignages de particuliers) les hackers qui peuvent être sollicités dans ces cas.

Entretien 26

| | |
|---|---|
| **Nom** | **EPELBOIN Fabrice** |
| **Date** | 08/04/2022 |
| **Fonction** | Entrepreneur dans le secteur numérique, enseignant du supérieur |
| **Expertise** | **Questions cyber, droits civiques, confidentialité en ligne, guerre informationnelle, hacktivisme** |

**Notion de « hacker éthique »**

Expression marketée inventée par IBM.

C'est un hacker qui travaille au service d'une entreprise et pas au service d'une cause morale. [une éthique n'est toutefois pas forcément liée à la morale, c'est une vision à vocation fédératrice].

Il respecte juste la loi.

Selon FE, la Loi pour une République numérique de 2016 n'en est pas vraiment une, mais une correction de dispositions « idiotes » préalables.

La question du hacking et des hackers n'est pas binaire : il n'y a pas de « gentils » ou de « méchants » hackers. Il faut aller chercher l'intelligence (le savoir-faire) entre les deux : chez les hackers gris dits « hacktivistes ». Ils ne respectent pas nécessairement la loi mais ils sont très compétents, et donc utiles pour le renseignement et ont de ce fait des contacts avec les SR d'Etat.

FE travaille donc avec eux (Olivier Laurelli par exemple de Reflets.info). Ceux qui ont piraté Bachar el-Assad dit-il, ceux qui dévoilent des scandales d'Etat ou privés, par exemple.

**Rapports entre autorités/politique et communauté de hackers**

Le contexte historique est négatif : « ça a mal commencé. »

Il y a un aspect culturel puissant : celui d'une défiance et d'un mépris initiaux des autorités françaises à l'égard des hackers. Il parle d'un environnement hostile et toxique pour les hackers. Aujourd'hui, du moins, on est en transition avec une rémission de cette culture toxique. Mais c'est la classe politique qui, selon FE, pose problème (ignorante et méprisante, à cheval sur ses privilèges établis donc hostile par nature à une culture alternative telle que celle du hacking). Et pas les SR qui emploient eux aussi des hackers et qui comprennent le langage et le savoir-faire de la communauté.

C'est par le logiciel libre et open source que la communauté s'est maintenue dans une certaine mesure en France. Mais aucun club/association de hackers n'a été créée en France qui aurait pu être un interlocuteur de l'Etat.

La France, selon FE, est très corrompue par les GAFAM.

Vu des hackers, c'est la déception, et ils considèrent que les autorités sont antipatriotiques.

« L'ANSSI fait ce qu'elle peut » face à cet environnement politique nocif.

En France, soit on attaque juridiquement l'Etat pour des lois « débiles », il y a plus de confrontation ; soit on ridiculise les hommes politiques car ils n'y connaissent rien.
On évoque Cédric O et sa promotion faite aux GAFAM et à NordVPN à l'assemblée par exemple, sous couvert de présenter aux députés ce qu'est un VPN…
FE parle de 4 ou 5 députés qui connaissent un minimum les questions numériques.

En Allemagne, par exemple avec le CCC (Chaos Computer Club), le premier vrai club de hackers structuré, c'est bien différent. Du CCC allemand a dérivé un CCC français à Paris, mais c'était un faux nez (honeypot) du renseignement français, dit FE, en vue de « scanner » l'écosystème du hacking dans le pays et les profils significatifs. Ce que la communauté des hackers française a eu du mal à digérer.

La vision amalgamant criminalité et hacking a longtemps prévalu en France (« il y a encore… disons 6 ans »). La culture pop/geek (BDL, Mr Robot…) a changé un peu ça.
Mais on est loin de l'Allemagne où cela fait un moment les hackers sont entendus, consultés et reçus. FE parle d'une véritable synergie avec l'Etat. Il y a eu de nombreux départs de hackers français en Allemagne du fait de cette culture délétère en France. Les représentations sur le sujet ont favorisé des vocations et crée un statut.
Le législateur allemand va voir les hackers au préalable, discutent avec eux, consulte leur point de vue. Il y a une vraie collaboration.
En France, il n'y a pas cette interaction. Mais des contacts entre Etat et individus. Pas de relations donc avec l'équivalent du CCC allemand.
Il y a des contacts avec les SR étatiques parce qu'il y a beaucoup de patriotes chez les hackers, mais c'est difficile à structurer car on passe juste par des individus.
Un certain partage de valeurs donc avec le RENS (pragmatique) et ça se passe malgré le politique.
FE évoque l'affaire « Bluetouff » (Olivier Laurelli, hacktiviste chez Reflets.info) comme représentative des intérêts et de la sanctuarisation de l'Etat français. Pendant sept ans, Bluetouff a connu un harcèlement judiciaire (évoque les « réseaux Sarkozy »). Les documents qu'il avait copiés depuis le site de l'ANSES (qui l'a poursuivi en justice) touchait des points sensibles et des questions politiques (M. Aubry).
Or, Olivier Laurelli aurait parallèlement selon FE de bonnes relations (collaboration) avec les SR français, du fait de ses réseaux et de ses sources d'information par rapport à plusieurs sujets (Lybie, Printemps arabe et d'autres théâtres d'opération).
En revanche, les relations avec les politiques sont exécrables.

FE évoque son arrestation de façade par la DGSE [DGSI ?] et sa mise en relation avec la direction technique>service cyber. Il était respecté à la DGSE dit-il.

Il y a des hackers à la DGSE, DGSSI, l'ANSSI [pas tout à fait le discours officiel/voire ce qu'en dit Xorg].
Ils sont recrutés soit par tamponnage, soit par casting efficace, soit par engagement plutôt militaire (vocation)
Si on veut être hacker avec un bon salaire, c'est plutôt comme ça.
La passerelle c'est l'ANSSI, l'armée, mais on est moins bien payé.
Les entreprises paient mieux mais les missions sont peu passionnantes, et ne traitent pas bien les hackers (sauf rares exceptions). Rapport utilitariste. Elles ne bâtissent pas grand-chose. Les hackers en sont bien conscients et jouent le jeu car ils sont très demandés.
En Allemagne, il y a plus de considérations mais le travail n'est pas non plus passionnant, donc il y a pas mal de mouvement (d'où le côté supposé « mercenaire » des hackers), et on va changer de boîte assez facilement.

En France, beaucoup de vocations aujourd'hui.
A terme cette génération va améliorer l'approche en termes de cybersécurité dit FE.
Et vis-à-vis des politiques, dans plusieurs années (une génération), ça s'améliorera possiblement, si on en finit avec les lois portées par les lobbies et les conflits d'intérêts politiques.
« L'Etat, au mieux, vis-à-vis du numérique, est un singe inculte maniant une AK-47. »

La classe politique a commencé à avoir peur et se méfier du cyber par ignorance et quand les affaires Wikileaks ont commencé (porte atteinte à l'Etat).
Il y a une vraie dualité entre la classe politique et les activistes/hacktivistes, « qui veulent la mort du système politique actuel ».
Ambivalence, car on les méprise mais on a besoin d'eux.
Tant que ce système/cette culture politique en France continuera, on aura cette défiance.
Mais ça pourrait changer avec la génération suivante.

Les médias français ne traitent toutefois plus de la même façon la question du hacking [malgré quelques extrapolations et biais liés à la complexité et au caractère fermé du hack // « darknet »…]
Il y a 5/6 ans en France, il y a eu un changement et cela suscite de plus en plus de vocations chez les jeunes (que les parents ne comprennent pas et même dont ils ont peur pour l'avenir de leurs enfants).

La culture française de « la fiche de poste » a commencé à s'atténuer, grâce à l'ANSSI.
EB cite le cas de Matthieu Suiche, hacker français qui a ralenti la diffusion du ramsoware Wannacry en 2017. « Il n'avait que le BAC ». L'ANSSI a voulu l'engager mais ne pouvait pas vu les statuts. Il travaille depuis à Dubaï où il a été accueilli comme il se doit…

En réalité, il n'y a pas de corrélation entre niveau de diplôme et expertise en hacking.

**ANSSI, COMCYBER**

G. Poupard a tapé du poing sur la table et demandé à ce que le COMCYBER s'ouvre de la même manière que l'ANSSI.

Entretien 27

| | |
|---|---|
| **Nom** | **KAZAR Yassir** |
| **Date** | 20/05/2022 |
| **Fonction** | Entrepreneur, co-fondateur et actuel directeur de Yogosha. |
| **Expertise** | **Cybersécurité, hacking** |

Yogosha est une plateforme qui organise de bug bounty et facilite ainsi la détection des failles, en mettant en rapport hackers et entreprises. Audit, pentesting, remontée coordonnée de vulnérabilités. C'est l'intention qui est prise en compte vis-à-vis des hackers.
Cadre : textes de loi, workshop USA-UE et loi pour la République numérique de 2016.

**Caractéristiques des liens hackers-entreprises**
Approche quantitative à privilégier pour appréhender le phénomène selon lui : nombre d'articles de presse, de hackers dits éthiques, de bug bounty proposés. En augmentation croissante.
Le sujet s'installe et bien que le cliché du hacker résiste, ils gagnent des prix, on les met en avant. Tendance qui s'installe surtout si l'on compare à la situation il y a encore cinq à dix ans.
Le recrutement, qui encore légitime le diplôme, commence toutefois à s'ouvrir à des profils atypiques, à minimiser le diplôme.

Conscience du risque cyber
Dans les grandes entreprises où on a au minimum un RSSI et un pôle sécurité.
Dans les PME ça avance doucement, il n'y avait pas de contrats avant.

Factuellement donc, dit-il, il y a des liens évidents.
Ces relations sont certes utilitaristes (mais c'est global, c'est le marché). Yogosha crée un marché pour les hackers.
D'un point de vue organisationnel, il y a sans doute à évoluer. Il faudrait que la sécurité informatique et numérique soit plus arrimée/dépendent au/du COMEX des entreprises, et plus du DSI. Un poste de DSSI serait-il une bonne chose Yassir Kazat se demande-t-il ?

**Liens hackers-Etat**
Allemagne/France. L'Allemagne est certes plus ouverte avec le CCC (Chaos Computer Club, qui s'est imposé), mais la relation suit une dynamique.
En France, selon lui, l'équivalent du CCC est l'association La quadrature du net, en lien avec la HackerzVoice (convention créée par Paolo Pinto « CrashFR » en 2001) qui organise la *Nuit du Hack*.
Une approche quantitative est là aussi à adopter selon lui : nombre de hackers et de programmes bug bounty et de CTF (exemple le 404CTF parrainé par la DGSE). Le Comcyber a lancé un bug bounty avec Yogosha.
Le Campus Cyber va dans ce sens. Il y a un Hacking Event, organisé très tôt. Il y a une place de plus en plus prépondérante qui est faite au phénomène.

Dans le domaine éducatif, sans être une structure étatique, l'EGE organise aussi des CTF.

Hack4values est une initiative lancée par Yogosha qui permet l'aide gracieuse de hackers au profit de structures.
On peut parler d'entraide, de collaboration, de partage de l'information, de technologisme (sic), de méritocratie.

Peut-on pour autant parler de structuration d'une communauté de hackers en France ? En vue d'être des protagonistes-clés dans la société française ? Quelle est la part de représentation des

hackers français ? Il manque selon lui un organisme de représentation, comme le CCC en Allemagne, qui a réussi à s'imposer comme tel, un vrai interlocuteur face à l'Etat.

Ca devrait sans doute venir de la communauté française du hacking selon lui, mais il n'y pas assez de groupes d'individus assez forts (avec un leadership portant des revendications sur la société et la politique) pour structurer la communauté.
Cela peut-il venir du Parti pirate ? (initiative). C'est lié à La quadrature.
Hackers sans frontières [cofondée par Florent Curtet, Clément Domingo…] ? Pourquoi pas, mais quelle dynamique réelle ? Mais elle a une vocation européenne, bien que ce ne soit pas contradictoire.
Il y a trois acteurs dans le bug bounty en France : les deux premiers sont français (Hack in Provence, association loi 1901, et La quadrature du Net).
Selon lui, ce n'est pas à l'Etat de le faire.

**Lien renseignement-hacking**
« L'OSINT ouvre la brèche de la décentralisation du renseignement. Tout le monde peut se l'approprier par la technologisation extrême (sic). Tout le monde devient son propre agent de renseignement. »
« Le métier du renseignement « se plate-formise », comme tous les métiers. » (sic)
« Syndrome du changement radical de nos sociétés. »

Entretien 28

| | |
|---|---|
| **Nom** | **SEJEAN Marc (interviewé par un de nos étudiants en école de journalisme, Tom Falguerolles)** |
| **Date** | 20/03/2023 |
| **Fonction** | Informaticien spécialiste en sécurité numérique. |
| **Expertise** | **Cybersécurité, hacking** |

C'est un travail bénévole, que les hackers n'ont pas toujours été prêts à fournir dit-il, mais pour Marc Sejean, les hackers d'aujourd'hui sont différents « *On est une nouvelle génération de hackers, la plupart sont patriotes et prêts à aider les TPE et les forces de l'ordre à sécuriser le pays* ».

La jonction entre le monde civil et militaire est, de nos jours, assez fine et cette nouvelle génération est prête à défendre aussi bien qu'à attaquer pour leur pays.
« *On aimerait aller plus loin, pouvoir attaquer ceux qui nous attaquent, peu importe le pays*». Cependant, il est de l'avis de Marc, qu'en France il est toujours complexe de passer réellement à l'attaque. « *En France c'est très compliqué, on est une démocratie, un état de droit, et on doit se battre contre des pays qui ont des structures moins monolithiques où il y a une perméabilité entre les services secrets, les mafias et les cyber criminels* ». La Russie fait, bien entendu, partie de ces pays ; le président russe a récemment reconnu que si les hackers de son pays effectuaient des actions « patriotes », il ne les pénaliserait pas.

« *Il n'y a pas un jour aujourd'hui où l'on ne subit pas une cyberattaque. C'est pour cette raison que la guerre traditionnelle a laissé place à la guerre informatique, l'espace et le cyberespace fusionnent désormais. Plus complexes mais moins manifestes pour le grand public, ces batailles de l'invisible sont menées par des professionnels de l'informatique. Tant en hard power qu'en soft power, le hacker est devenu le bras armé invisible des Etats-nations.* »

Entretien 29

| | |
|---|---|
| **Nom** | **HAJRI Sylvain** |
| **Date** | 27/02/2023 |
| **Fonction** | Chef d'entreprise, co-fondateur de osintfr.com, communauté d'intérêt sur l'OSINT et fondateur d'epieos.com |
| **Expertise** | **Cybersécurité, OSINT, entrepreneuriat** |

Autodidacte qui a commencé par apprendre l'informatique et débuté l'OSINT en 2010. Il vient de la cybersécurité et travaillé comme indépendant pour des entreprises dans le risk management (notamment chez Orange).
Quand il commence à pratiquer l'OSINT, il ne connaissait pas l'acronyme et entendait parler de reconnaissance passive (qui est le nom souvent usité désigner la première phase du pentesting) voire de « stalking », qu'on utilise encore aujourd'hui, mais de manière erroné quant à sa vraie signification littérale.
Il a eu l'idée de créer un CTF (*capture the flag*) en associant du redteaming à un évènement reconnu de hacking physique (lockpicking notamment, « piratage » de serrure) baptisé le *Gringo Warrior Challenge*. Cela donnera le *Spying Challenge* (https://spyingchallenge.com/), cofondé avec Mélik Lemariey et Christophe Baland.
Ensuite, il a récupéré une chaine Discord fondé par « Choucroute » et en a fait un site web appelé osintfr.com. L'objectif était/est de favoriser une communauté de pratiques et de partage en vue de fédérer les sphères journalistique/policière/hacking/cybersécurité/intelligence économique.

En 2020, après avoir créé epieos.com il a exprimé le désir d'être mis en relation avec les autorités françaises, et également les entreprises BtoB (2017). Du côté de l'Etat, pas de réponse ; du côté des entreprises nationales, quelques-unes ont manifesté leur intérêt, mais peu.
Avant le déclenchement officiel de la guerre d'Ukraine en 2022, il avait proposé des bulletins de veille OSINT sur le conflit [alors qualifié de « basse intensité »] à des entreprises de défense/sécurité ou ayant des filiales en Ukraine et Russie. Ça n'intéressait personne, mais on l'a recontacté a posteriori.

### Caractéristiques des liens hackers-Etat

Selon lui, il y a plein de bonnes volontés pour réunir les deux mondes, mais il évoque le « copinage » qui gangrène ces interactions. Il mentionne comment il a pu, dans le cadre de *l'OSINT village* de l'évènement *Le Hack*, invité des fonctionnaires de police, des militaires, etc. Sans ce biais-là, il ne serait pas parvenu à les rencontrer.

Selon lui, en France il y a une créativité qui est entravée dans ces domaines. Il évoque la situation en Israël et ces entreprises qui sont créées par d'anciens militaires et/ou de l'unité 8200 de Tsahal. Lesquelles ne sont pas forcément toutes sulfureuses et même ont pignon sur rue et jouissent d'une excellente réputation (ex : Checkmarx).
Il évoque le paradoxe d'avoir des clients très très largement dans des pays étrangers et non français : américains, canadiens, australiens notamment). Par exemple, il a été invité par Interpol pour mars 2023 au siège de l'organisation à Lyon, mais par des policiers australiens (questions liées à la pédo-criminalité)

**Lien renseignement/OSINT-hacking**

Deux philosophies selon lui :
Il y a les journalistes d'investigation qui font de l'OSINT (Openfacto, équivalent français de Bellingcat, l'AEGE aussi dans une bonne mesure), et les OSINTers-hackers, qui ont une culture plus technique et cybersécurité (philosophie de osintfr.com) et ne souhaitent pas être politisés. Lui-même ne souhaite pas forcément être en rapport avec l'Etat vis-à-vis d'Epieos (qui commence à bien marcher commercialement parlant selon ses dires). Donc ne souhaite pas de politisation de son service [et sans doute garder le contrôle sur son business].
En France, la communauté OSINT est très bien représentée avec beaucoup de spécialistes, elle jouit même dit-il « d'un soft power ». Mais il interroge la place des institutions françaises : suivent-elles le mouvement ?

« *L'OSINT, c'est comme la tech dans les années 90. C'est du bricolage.* »

**A-t-il reçu du soutien de la part de la sphère privée ou de l'Etat pour osintfr.com ou epieos ?**

Non, et il veut rester indépendant. Osintfr.com est une communauté informelle, même pas une association dit-il. Mais ses invitations à des gendarmes ou autres sont quand même honorées. Et c'est ça qui, pour lui, montre un intérêt (mais encore « complexé »).

Par ailleurs, quand il a fondé epieos, on a voulu lui nuire et faire capoter son projet. Selon lui : des concurrents étrangers (Anglosaxons et Israéliens) mais aussi français. Il a identifié des velléités/un projet de campagne de dénigrement qui serait passer par le média spécialisé *Intelligence Online*.

Personnes-clés évoquées :
Le juriste et RSSI Marc-Antoine Ledieu, et Jean-Marc Manach, journaliste d'investigation.

Entretien 30

| | |
|---|---|
| **Nom** | **« Alice » (anonymisée)** |
| **Date** | 01/03/2023 |
| **Fonction** | Gestion de projet, entrepreneuse, développeuse blockchain, spécialiste de l'analyse de données et de la blockchain. |
| **Expertise** | **Hacking, Big data, OSINT, Blockchain, hacktivisme** |

### Caractéristiques des liens hackers-entreprises

Le problème de la France selon elle : « l'ingérence du système » ou hors système ». Plusieurs forces s'opposent. Pas facile de faire bouger les lignes. Il y a une certaine paranoïa. On ne veut pas prendre de risques. Les autorités ne voient pas le potentiel.
La législation française est *punitive*, la législation américaine est *négociatrice* (avantage/faiblesse, rapport coût/bénéfice typique d'une culture capitaliste forte)

« Quels hackers ? » : « de qui parle-t-on », demande-t-elle ? Les « hackers blancs » ne sont pas des hackers selon elle. Les activistes ne peuvent pas être « blancs. »

### Liens hackers-Etat

Bien qu'elle ne souhaite pas être caractérisée, elle s'apparente à une hackeuse grise.
Ses liens : elle dit être « cramée » (elle a subi des perquisitions à son domicile…) auprès de l'Etat. Elle a touché à des « dossiers sensibles » et on lui a « envoyé un message/des messages » (elle a « un casier judiciaire vierge par exemple ». (*sic*), elle dit avoir été l'objet de plusieurs filatures. Elle préfère ne pas trop en parler, car « tout n'est pas terminé », et qu'il y a encore des problèmes potentiels avec d'anciens protagonistes… qui seraient connectés à la DGSE. Elle a identifié cela en faisant de l'OSINT sur elle-même.

Elle évoque le jeu de pistes « Cicada 3301 » fondé en 2012 sur le besoin d'identifier des profils de haut potentiel (pour les recruter) dans l'informatique en général, de la cryptographie et de l'OSINT en particulier. Selon elle, ce n'est pas la NSA, pas les Etats-Unis qui sont derrière. En creux, elle semble vouloir implicitement indiquer qu'il s'agit peut-être de la France. Et ça continuerait.

En 2013/2014, lors d'une phase de candidature/recrutement de la DGSE et de la DGSI, on l'aurait tamponnée pour une mission portant sur une analyse de gros volumes de données. Elle dit avoir été contactée par « un responsable du bureau des affaires réservées du MININT » (*sic*). Sa mission : on lui demandait si elle était en mesure de faire de la data science sur un volume de « 67 millions de gens » (*sic*).

### Rapports police / hackers

Les hackers sont suspects par défaut, « et c'est normal » dit-elle. En rapport avec eux, elle doutait de leur honnêteté. Ne savait pas si on essayait de la piéger ou si les rapports étaient sains. « On te change de statut », fait-elle remarquer.

Certains hackers (gris, hacktivistes) sont sortis de la sphère du hacking parce que c'était dangereux.
« Les autorités peuvent monter un dossier sur toi pour te charger. »

Elle dit seulement vouloir « comprendre ». Et donc faire de la collecte d'informations « pour assembler le puzzle. »
Elle a été invitée au salon de la Blockchain au MININT. Quelqu'un du ministère ne savait pas si c'était vraiment elle ou pas (autrement dit si elle était sous pseudonyme sur le web ou si c'était sa vraie identité).

**Lien renseignement/OSINT-hacking**

L'OSINT est ambigu, à partir du moment où tu fais de la corrélation de données, et dépend beaucoup de l'utilisation qui en est fait.

**Comparaison avec d'autres pays**

La nouvelle loi sur le hacking en Belgique est une accélération de la cyberguerre à ses yeux. C'est une sorte de rets lancés aux gros poissons, il y a derrière cette posture une espèce de logique de recrutement des « bons ».
En France, la Loi pour la République numérique de 2016 montre que les institutions ne te protègent pas si tu ne te protèges pas toi-même.
Cette loi montre qu'il y a des précautions énormes à prendre (juridiques notamment).
Et c'est aussi comme une phase de recrutement pour les entreprises.

Entretien 31

| | |
|---|---|
| **Nom** | **LAURELLI Olivier ("Bluetouff")** |
| **Date** | 30/03/2023 |
| **Fonction** | Journaliste d'investigation/Cofondateur de reflets.info ; hacker/informaticien autodidacte |
| **Expertise** | **Hacking, cybersécurité et confidentialité/privacy, OSINT, hacktivisme** |

Deux niveaux de RENS selon lui en France :

- Les services
- Le MININT

Il est surtout connu, à son corps défendant (ça lui a nui jusqu'à maintenant déplore-t-il) pour l'affaire liée à son pseudo, « Bluetouff ».

Il a été inculpé, on l'a perquisitionné et on a analysé ses matériels informatiques dans ce cadre. C'était en 2015.

Lors de son procès, il a fallu consacrer le « vol de données », car le droit français était inopérant jusque-là sur cette question de vol d'objets « immatériels ». Il a été accusé de s'introduire dans un espace public (le site web de l'ANSES) et avoir volé des données. Il écopera d'une amende de 3000 euros.

Il a connu d'autres condamnations mineures. On l'avait aussi interrogé car il était l'objet d'inquiétudes à propos de ses enquêtes sur la société française Amesys, qui a commercialisé des solutions logicielles de surveillance (interception des communications IP – logiciel *Eagle*) notamment à la Lybie de Kadhafi puis à l'Egypte d'Al-Sissi (société rebaptisée Nexa technologies).

Il a travaillé pour le compte de l'Etat, plus ou moins directement puisque l'entreprise (Société coopérative d'ingénieurs experts du logiciel libre pour hébergement/infogérance et devops) où il travaillait alors (Bearstech, toujours existante) avait en charge l'hébergement des données de l'Elysée.

Il a été hacktiviste contre la Russie. On connaissait ses réseaux humains assez développés, notamment dans des régions qui pouvaient intéresser l'Etat français (pays arabes/ Maghreb). Il a beaucoup couvert les Printemps arabes de 2011. Mais il indique que l'Etat ne lui a jamais confié de missions en dépit de ses « entrées ». Des éléments de ses réseaux ont toutefois, eux, été contactés, lesquels ont décliné.

Il était toutefois en rapport avec la DCRI à l'époque, et a gardé le contact avec deux désormais anciens policiers du service.

**Relations avec l'Etat, question des communautés de hackers.**

Le vrai problème, selon lui, est la « corruption des hommes politiques français » (sic). Même des policiers ont déploré l'acharnement contre lui lors de l'affaire Bluetouff (« on a perdu notre temps avec Olivier Laurelli. » a-t-il entendu de leur part)

De fait, les hackers sont perçus comme une menace par les autorités.

Il y a un niveau historique et culturel de défiance. C'a commencé avec le « Chaos Computer Club français » (en fait, un subterfuge de la DST, désormais bien connu et documenté). C'est l'événement traumatique des rapports entre autorités et hackers.

D'après lui, la communauté des hackers s'est alors divisée et beaucoup d'entre eux ont pris peur et sont allés vers la communauté du logiciel libre. Contrairement à ce qui s'est passé avec l'originel et authentique Chaos Computer Club (CCC) allemand, qui n'a jamais été un cheval de Troie des services de renseignement allemands.

Il stigmatise donc une inculture de la classe politique française et de la Justice vis-à-vis du numérique.

Il  m'oriente vers Marc Rees, fondateur du média Next Impact.

Entretien 32

| | |
|---|---|
| **Nom** | **MANACH Jean-Marc** |
| **Date** | 10/04/2023 |
| **Fonction** | Journaliste d'investigation indépendant, spécialiste d'OSINT. |
| **Expertise** | **Journalisme d'investigation, OSINT, culture du cyberespace** |

Il a eu des liens avec les SR et les hackers dans les années 2000.

Il raconte l'histoire ancienne de la réflexion de l'armée sur les questions de sécurité numérique et la guerre électronique, au sein de l'École supérieure et d'application des transmissions (ESAT) aujourd'hui *École des transmissions* (ETRS). Les origines du FIC, notamment, sont le SSTIC (Symposium sur la sécurité des technologies de l'information et des communications) qui s'insérait dans l'ESAT. Le SSTIC a été créé par un ami d'Eric Filiol (ancien cryptographe dans l'armée), Frédéric Raynal (revue MISC, QuarksLab, Reflets.info)

Le milieu militaire s'est tôt intéressé aux hackers.

Me conseille le documentaire qu'il a coécrit sur la contre-histoire d'Internet pour comprendre le rapport hackers/autorités. C'est très important pour appréhender la situation aujourd'hui.

https://vimeo.com/311894477

Recontextualisation de la naissance du Chaos Computer allemand, le plus ancien CCC et le plus solide.

J-MM évoque la guerre froide et l'IDS (Initiative de défense stratégique connue sous le nom initiative « Star Wars » ou guerre des étoiles). C'est une opération psychologique (psyops) lancée par les USA pour tromper l'URSS. Quatre Allemands du CCC ont été employés par la Stasi pour comprendre la teneur et la nature de l'IDS.

En France, le CCF (CCC français), Chaos Computer France, est créé par la DST comme cheval de Troie pour identifier les hackers nationaux. Donc, on ne prétendait pas hacker, c'était tabou, parce qu'on savait qu'on serait suivi par les SR.

La DST était en train de s'informatiser et faisait appel à des étudiants en informatique parfois hackers venant faire leur service militaire.

Fin des années 2000, Philippe Langlois organise un *Hacker Space* en France, les hackerspaces sont des laboratoires communautaires ouverts où les hackers peuvent partager leurs ressources et leurs connaissances.

https://www.tmplab.org/

https://hackerarea.wordpress.com/

Selon JMM, l'ANSSI a siphonné le marché de la cyber.

Au sein du SSTIC, se trouvait la RSTACK, groupe de hackers français brillants (dont est issu Laurent Oudot, cofondateur de TETHRIS et ancien de la DGSE)

Les relations entre DST et hackers se sont mal passées dans les années 90, mais plutôt bien passées avec la DGSE dans les années 2000. Au moment où Bernard Barbier, DT de la DGSE arrive et en recrute, conjointement avec la « Baleine » (nom de code du général Jean Guyaux détaché à la DST).

JMM indique que ce sont des civils comme Barbier qui ont permis l'arrivée de hackers à la DGSE. Ces civils ne voulaient pas séparer la direction technique du renseignement.

Aujourd'hui, on voit pas mal d'offres d'emploi de la DGSE recrutant des offensifs (redteaming, pentesting…), la DGSI et le SCRT des osinters. DRM, DRSD et DGSI se rapprochent de sociétés spécialisées dans l'OSINT. Pas la DGSE a priori. JMM se base beaucoup sur les offres d'emploi qu'il suit assidûment.

La DGSE fait du cyber offensif depuis le Fort de Noisy, propriété du MINARM. En outre DGSE et DGSI travailleraient selon JMM à élaborer des spywares.

JMM a planché sur la BdD de Strava lors de l'affaire baptisé à partir du nom de ce service applicatif de métrique de performances sportives. Il avait trouvé les données du n°2 de la DGSE, qui l'avait contacté plus tard au sujet de son travail de factchecking des unes du Monde.

JMM évoque de la culture de l'information de la CIA, alors que les SR français ne communiquent pas.

Evocation des usages duaux des TIC. Avec Chaouki Bekrar qui, en France, est le premier à avoir fait du *full disclosure* sur les données fuitées. Français d'origine marocaine, la DST l'avait appréhendé, et il était alors parti en 2015 aux USA pour créer sa société Vupen Security, flanquée de sa plateforme d'acquisition d'*exploits* de faille « zero day », Zerodium. Il est aujourd'hui l'un des principaux fournisseurs de failles « jour-zéro » aux USA.

Du côté de la classe politique, il y a un vrai problème de culture et de connaissance en termes de cyberespace au Parlement par exemple.

Les rares qui maitrisaient le sujet ont été balayés dit JMM.

JMM me fait la proposition de recenser les spécialistes d'OSINT dont moi pour peut-être créer une communauté plus formelle et unifiée… (reprendre contact avec lui après le doctorat…)

JMM m'oriente vers Guilhem Giraud (ancien de la DST) qui a créé une plateforme d'OSINT (Temno), Mathieu Amiot (tous deux dans mes contacts LI), également chez Temno.

Contacter des anciens de la RSTACK comme « Newsoft » (Nicolas Ruff), Christophe Boutry (ancien policier), surtout pour l'OSINT.

Entretien 33

| | |
|---|---|
| **Nom** | **POUPARD Guillaume** |
| **Date** | 17/04/2023 |
| **Fonction** | Ancien directeur de l'ANSSI, directeur adjoint de Docaposte. |
| **Expertise** | **Cybersécurité & cyberdéfense** |

Il y a encore quinze ans, l'approche à l'ANSSI et en France en général était très « MININT » (ministère de l'Intérieur), très silotée.

Les hackers étaient vus comme nocifs, dangereux. On était à envoyer « des fourgons de police » lors des éditions de la *Nuit du hack*. « *C'a évolué aujourd'hui. L'Etat est monté en conscience et compétence.* »

GP parle d'une belle évolution dans la perception des choses (nécessité), pour l'échange, la coopération. On ne cherche pas forcément à savoir d'où viennent les infos.

Après, la question est : il y a ceux qui respectent la loi et les autres. GP dit qu'il a ouvert au maximum autour de l'écosystème mais a fixé une ligne rouge avec les gens non respectueux de la loi.
« *Or, la loi française est très stricte. Donc un chercheur en informatique est toujours limité. Car ce n'est pas un "blanc" pur.* »

Amélioration donc : Passer par des intermédiaires. L'ANSSI comme le MINARM utilisent les plateformes de bug bounty. Rapprocher les compétences, avoir une bonne image pour le recrutement (ça passe beaucoup par les connaissances). Donc s'ouvrir à tout l'écosystème cyber, à la communauté open source, l'enseignement, tant qu'ils ne franchissent pas la ligne rouge. Ils se rencontrent tant qu'ils ne passent pas cette ligne.

**Rapports concrets avec hackers/l'écosystème open source**

Ça prend du temps. Et, oui il y a un côté « utilitariste ». « *En bon technocrate dit-il, ça ne choque pas. On veut le plus utile et efficace. Mais c'est dommage car c'est du court-terme. On a toujours peur d'être manipulé quand on ne vient pas du sérail. D'où toujours une méfiance.* »
Il n'y a donc pas de structuration, alors qu'avec le Chaos Computer Club, ça existe en Allemagne. La *Nuit du hack* pourrait jouer ce rôle avec les plateformes de bug bounty.

Donc pas de liens directs mais des résultats transmis, comme avec le cas Florent Curtet. Il est intéressant de ce point de vue. Mais côté parquet/Justice, ils ne sont pas contents.
Il y a malheureusement très peu de juges spécialisés dans les questions cyber.

GP corrobore le point de vue de bien d'observateurs sur l'affaire « Bluetouff ». « *A l'ANSSI, dit-il, dès le début on avait des plaintes déposées pour des scans de ports.* »
C'est exagéré.
Aujourd'hui il y a une meilleure compréhension malgré tout.

**Comparaison avec d'autres Etats**

Le débat en Belgique, et la nouvelle loi sur l'évaluation libre des failles de sécurité, font peur en France. On redoute l'effet d'aubaine que ça peut générer, et qui bénéficierait aux criminels.

Ex. : la loi pour une République numérique de 2016 en France : la nécessité d'anonymiser ou pas les remontées de failles est très discutée. La loi dit que l'ANSSI n'est pas obligée de dénoncer de telles alertes. Mais le niveau d'équilibre en France n'est pas trop protecteur pour les gens honnêtes.

« *La loi pour la République numérique de 2016 ne légalise pas formellement le hacking éthique.* »

De plus, les éditeurs n'aiment pas le full disclosure, donc d'autres pays vont plus loin. On pense que plus on va protéger les hackers, plus on va a avoir un effet d'aubaine. L'équilibre pourra peut-être évoluer en France. Il faut au moins éviter les erreurs judiciaires.

Pour revenir à la LPRN de 2016 : le terme « lanceurs d'alerte » pour désigner les hackers, ça parlait aux parlementaires. « *Ça montre la méconnaissance, et tous les textes sur le numérique, c'est pareil. Les parlementaires n'ont pas la culture numérique*. »

GP évoque Axelle Lemaire, ancienne Secrétaire d'État chargée du Numérique et de l'Innovation sous F. Hollande, qui selon lui comprenait un peu les enjeux du numérique, mais pas vraiment ceux de la sécurité du numérique. Il ne fallait pas mélanger les deux.

« *Il y a donc un gros travail de pédagogie à faire auprès des élites politiques*. »

Au bilan, on préfère que ce soit globalement interdit, sauf avec des gens honnêtes. C'est l'équilibre auquel on est arrivé en France. Avec une Justice qui est très frileuse pour changer des choses dans la loi.

**Services de renseignement et hackers**

La posture des SR est de limiter les risques Leur état d'esprit c'est ne pas jouer avec ceux qui dépassent la limite. Il y a une peur des risques de scandales. Il faut parler avec l'écosystème, même par « utilitarisme ».
« *Mais il n'y a pas de tout blanc ou de tout noir chez les hackers. Mais il y a des limites à ne pas franchir.* »

« *D'un autre côté, chez les hackers eux-mêmes, ceux qui refusent la catégorisation* [black/grey/white hats], *ils jouent un jeu extrême.* »

GP confesse l'échec sous son mandat quant au recrutement, resté façon « fiche de poste ». Il regrette de ne pas avoir de faire avancer les mentalités et les usages (garde-fous administratifs) et donc permis le recrutement de profils atypiques, d'autodidactes. Quant aux profils classiques (type école d'informatique), « *on sait les recruter mais pas les payer.* » Cas où certains étaient déçus sur ce point. GP pense que ça évoluera. Le simple fait d'avoir des contractuels n'est pas évident. [A ma remarque : l'ANSSI avait donc tout de même initié le recrutement extérieur et en partie réussi, GP acquiesce.]

Il y a d'ailleurs quelques profils offensifs à l'ANSSI, les auditeurs (surtout en rétro-ingénierie). Il dit espérer que les autres services de l'Etat ont plus de facilité à les recruter. Il précise justement que la règle d'or avec les services offensifs, comme la DGSE, c'est de ne pas savoir ce qu'ils font.

Entretien 34

| | |
|---|---|
| **Nom** | **LAMOURI Karim** |
| **Date** | 07/07/2023 |
| **Fonction** | Entrepreneur, consultant SI (ancien technicien/administrateur/architecte/ingénieur systèmes), président de Hackers without Borders (HWB) |
| **Expertise** | **Informatique, sécurité informatique, cybersécurité** |

« *La France est une idée avant d'être un pays*. »
La France souffre d'être le peuple qui a le plus de besoin d'émancipation mais qui dans le même temps sait s'esclavagiser lui-même.

« *Or, comment hacker le cerveau d'un Français ?* »
C'est un pays qui performe dans les idées, qui crée des concepts.

**Relations Etat-hackers**

Son point de vue factuel : beaucoup de situations handicapantes pour les individus dans notre pays.
Il y a une arrogance extrême de nos élites politiques. Ils ne s'engagent en politique que par intérêt, pour des mandats. Il n'y a pas de noblesse dans leur engagement supposé.

Notre société, numérisée aujourd'hui, c'est agencer l'informatique, l'énergie et l'humain.
Il faut donc déjà commencer à protéger l'énergie (convictions pro-nucléaires) pour régir l'informatique et ses infrastructures.

Il y a un rapport biaisé avec les autorités. Pourquoi les hackers apportent leur aide et sont souvent patriotes : plusieurs facteurs, c'est un investissement social, psychologique, un besoin de sentiment d'appartenance, d'adhésion, une volonté (si connecté) de faire partie d'un réseau (social), au-delà du patriotisme.
Ils aident pour exister.

Mais il y a des rapports de pouvoir et d'argent dans la cybersécurité. Il cite par exemple les liens d'intérêt (y compris financier, participation…) entre l'Etat et Orange Cyberdéfense.

Il propose ses services au nom de l'ONG HWB à l'ANSSI, mais l'actuel directeur (Vincent Strubel) ne lui répond pas. C'est un pur produit de l'administration dit-il, qui a fait presque toute sa carrière à l'ANSSI.

*Or* « *le hacking, la sécurité c'est un état d'esprit*. »

Malgré ses efforts, Guillaume Poupard, l'ancien DG de l'ANSSI, est le parfait exemple que l'Etat reste l'Etat dit-il, et que ça ne changera pas.
On lui dit souvent : « pourquoi tu te fais chier avec ça, on admire ta volonté, mais reste où tu es ».

« *Si on attend des autorités qu'elles bougent, on est morts*. »
Il évoque l'immobilisme de l'Etat : « *Selon la définition du fou par Einstein, on est des fous. On fait tous les jours la même chose. Et on ne change pas*. »

L'ANSSI n'est pas une agence de terrain selon lui.
La directive NIS2 va faire bouger des choses mais pas avant 5 ans.

Ce que fait Nathalie Delattre, c'est bien. Proposer un OS (système d'exploitation) français souverain, c'est bien, mais il faut s'occuper des bases : par exemple quand on utilise des clouds américains, ça ne sert plus à rien, idem pour les smartphones.

Entre les acteurs de terrain et l'Etat, les relations sont nulles.

Ou alors, c'est du copinage et de la communication. Comme pour Hack4values : ils discutent avec Jean-Noël Barrot (actuel ministre délégué chargé de la Transition numérique et des Télécommunications) et les députés, mais ils font de la diplomatie, c'est du copinage.

Il dresse un tableau très noir de la classe politique. Il avance qu'au niveau des élites politiques, il n'y a pas d'intérêt à défendre la nation. Mais seulement « à se placer », avec leurs familles et leurs proches.
« *Il n'y a pas de lumière.* »

« *En France, l'image du hacker éthique, c'est un peu comme si on disait que c'est un "violeur sensuel".*»

« *Le salut viendra de la province !* »

**Relations hackers-entreprises**

Les entreprises ont compris qu'il y avait un intérêt pour la sécurité.
Mais l'historique houleux de leur rapport avec l'informatique fait qu'elles voient ça comme une fonction, et encore souvent comme un coût. Souvent c'était le DAF qui s'occupait de l'informatique. Sans parler des TPE même aujourd'hui.
C'est quand elles ont compris qu'on pouvait en tirer parti commercialement qu'elles ont compris l'intérêt de l'informatique. D'un coût on est passé à un gain.
« *Pour la sécurité informatique, c'est encore plus difficile. Les données et a fortiori les données personnelles, ça leur passe à côté.* »
C'est un investissement donc il y a deux écoles, les entreprises qui investissent et comprennent qu'il faut anticiper et être résilient, donc comprennent que c'est un investissement et pas un gain direct ; et les autres.

Dans le public : 2,5 à 3% du budget est consacré à l'informatique/sécurité (budget investissement et fonctionnement)
Dans le privé : 10% est consacré à l'informatique/sécurité. Ce qui est beaucoup.

Fameux adage, la question n'est pas de savoir si on va être attaqué, mais quand. Ca fonctionne. L'attaque tout le monde la vivra, surtout avec la montée en puissance et la maturation future de l'IA.

Des besoins sont exprimés par des entreprises avec lesquelles HWB peut être en rapport, mais pas officiellement et plutôt en réaction à des crises et non en anticipation. C'est dans une logique de rapport à un particulier, qui a besoin d'aide, que HWB agit.
Il explique que ce n'est pas la vocation de HWB et qu'il les oriente vers des boites françaises dont c'est l'offre (il cite l'exemple de Wallix).

Il cite Hexatrust (association qui essaie de fédérer les acteurs souverains et européens de la cyber), qu'il désigne comme le mélange ente le MEDEF et la CPME de la cybersécurité.

**Que pense-t-il du Campus Cyber ?**

« *C'est un bâtiment. Ça canalise un temps les forces vives. C'est un projet immobilier. Ce n'est pas essentiel. Faire la tournée des hôpitaux et des entreprises de France en quête de leurs besoins et de leurs vulnérabilités, ça c'est essentiel.* »

« *En France, on s'ignore : on ne connaît pas les forces qu'on a. Synacktiv, qui a piraté Tesla, c'est bien beau, mais on focalise sur les évènements « com ». C'est une goutte d'eau. Donc on ne connait pas.* »

https://www.synacktiv.com/

Il cite Sun Zi à ce propos :

« *Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites.* »

Pour KL, c'est la synthèse qui caractérise bien la France.

Entretien 35

| | |
|---|---|
| **Nom** | **PENALBA Pierre** |
| **Date** | 07/07/2023 |
| **Fonction** | Policier à la retraite (chef de cellule cybercriminalité à la PJ de Nice), spécialiste de cybersécurité et de hacking. |
| **Expertise** | **Cybersécurité, cybercriminalité, hacking** |

Fraichement retraité de la police, vient de publier l'ouvrage *Darknet, le voyage qui fait peur. Du fantasme à la réalité.*

**L'affaire Florent Curtet**

Au début, dit-il, ç'a été un « contact viril » puisqu'il se sont rencontrés réellement à l'occasion de son arrestation en 2007.
Début de l'affaire (criminelle) compliquée. Parce qu'il ne s'agissait pas du profil criminel type.

Juste un jeune gamin qui avait trouvé une faille dans le système pour se faire plaisir, briller et se faire une place socialement, auprès de ses amis notamment. Pas question d'un criminel chevronné.

Il évoque les méthodes de la police concernant ces profils :
Deux méthodes, soit c'est la case justice, soit on essaie de le recruter. On cherche le moyen de l'exploiter car il a une place ultra-privilégiée en termes d'accès à des informations-clés/difficiles à obtenir. En effet, c'est un profil particulier car connu/reconnu des autres hackers, donc il a accès à des informations de première main.

Donc, on recrute en fonction du niveau du profil.
Utilisation/manipulation des données et position (acheteur) dans un black market.

Pour Florent Curtet, je l'ai donc fait recruter, et il a en effet « travaillé » pour nous. Pas de travail rémunéré dans son cas. Il le faisait bénévolement.
Il était déclaré en tant qu'indic. Normalement on peut rémunérer les indics mais la procédure est compliquée et pas du tout dans un cas normal pour le cyber. Donc un indic dans le cyber c'est très neuf, et de fait il n'y a pas de procédure spécifique, d'où la plus grande difficulté encore qu'en temps normal.

Lors de sa 2e arrestation, Florent Curtet continuait de fournir des renseignements à la police (à PP) sur les groupes de hackers et les fuites de données. Ils profitaient de sa position d'interlocuteur privilégié avec les groupes cybercriminels est-européens. Il négociait à titre gracieux pour arranger/le bénéfice des entreprises françaises.

« *Mais à un moment il y a des collègues, et une procureure voulant faire du chiffre* (sic) » qui ont voulu lui tendre un piège selon PP. Les collègues en question, dit-il, c'est l'OCLCTIC et une unité spécialisée de la police de Lyon). Pour la procureure, c'est politique. Ça lui permettrait une promotion.

PP trouvait que c'était anormal que FC ne soit pas rémunéré. Et il l'a justement incité à en faire la demande. PP dit qu'il se sent donc un peu fautif, puisque c'est ce qu'il a fait arrêter dans une bonne mesure. D'avoir voulu être rémunéré pour son intercession de haut niveau en réalité.
Le piège vient du fait que, lors de l'affaire du cabinet d'avocats piraté, des policiers infiltrés (l'OCLCTIC/unité lyonnaise donc) se sont fait passer pour des avocats du cabinet. Ce sont les cybercriminels qui donnent le nom de l'intermédiaire avec qui il faut traiter. Ici, c'était FC. Donc les policiers sous couverture l'ont sollicité au nom du cabinet d'avocats.
PP dit que rien dans le dossier ne va contre FC. Et que l'affaire/la 2e arrestation accouchera sans nul doute d'une souris, d'un non-lieu. FC n'est pas à l'origine de la fuite, encore moins de l'attaque, et n'est pas à l'origine de la demande de négociation. Il ne voulait pas au début du reste.
PP dit que FC se sent coupable de quelque chose pour laquelle il ne devrait pas.

C'est PP qui a fait recruter FC à la DGSI, en parallèle de la candidature de ce dernier à un poste d'opérateur cybersécurité publique provenant de la DGSI. Il a donc d'abord été recruté comme « source », en fait « honorable correspondant » dit-il par l'affirmative à ma référence.
Mais le hacking et l'infiltration, c'est la 2e étape. C'est à celle-là que voulait se hisser FC. Il est donc passé à cette phase et a été rémunéré. Il l'évoque dans son livre.

**Travail de la police face à la cybercriminalité**

PP parle de son ancien travail : sur ces affaires d'infiltration, on travaille comme les SR, sous légende/anonymat, et on infiltre les milieux du darknet. Jusqu'à utiliser des méthodes illégales pour arriver à leurs fins. Il évoque l'anecdote personnelle d'avoir utilisé un cheval de Troie contre un cybercriminel pour récupérer des données pouvant l'identifier.
PP a participé à des opérations d'infiltration (missions spécifiques) et notamment il évoque les difficultés même sous couverture. On est hacker, on ne fait pas semblant de l'être. Ça se repère vite. On nous demande de faire nos preuves, et ça passe par des choses illégales. Anecdote : on lui a demandé de pirater un département du ministère de l'économie (que les cybercriminels en question avaient pénétré) pour juger de ses compétences et évaluer le niveau de confiance qui pouvait être attribué à PP. Il faut montrer patte blanche. Bien sûr, là le risque est trop grand et on joue avec la limite, puisque c'est illégal. Donc certains outrepassent mais pas la police, seulement certaines branches de la DGSE (surtout) et DGSI [cellule Richelieu ?].

PP a fait des passages/a travaillé avec la DST/DCRI/DGSI. Il a d'ailleurs été partie prenant et en même temps contradicteur du projet de Chaos Computer Club français (cheval de Troie pour attirer les hackers de l'époque)

**La police et les SR face aux hackers**

« *Tous les profils de hackers sont un peu bizarres.* »
Jamais tout blancs ou noirs. C'est une vision binaire qu'on a souvent.
On ne peut pas les surveiller 24/24.
Il y a un niveau de suspicion permanente notamment pour la police et la gendarmerie.

Oui, c'est un usage utilitariste de leurs compétences. Il n'y a pas d'affect. Avec des niveaux de sensibilité : gendarmerie un peu « humaine » plus que dans la police, et à la DGSI un peu plus qu'à la DGSE. « *A la DGSI, vous êtes un objet. A la DGSE c'est encore pire : vous êtes jetable.* »

« *A la DGSE, c'est zéro affect. Ce sont des pions jetables. Dès qu'on a plus besoin d'eux, on les lâche.* »

Ce que l'on fait dans la police, c'est qu'on essaie de retourner les gens qu'on arrête. On utilise la menace judiciaire et financière. Même avec toutes les ressources du monde et les meilleurs profils, on ne pourrait rien sans l'infiltration et les infos qu'on peut en tirer. Les « gris » sont la bonne interface (comme FC). Il faut des indics.
Il y a des tensions entre services, des luttes intestines. C'est une question de politique. Une affaire cyber appelle généralement toujours deux autorités : l'OCLCTIC (police) ou la gendarmerie. Il y a de vrais rapports de force. PP Cite une anecdote où on se jauge et on rabaisse l'autre service, façon cour d'école. Il évoque le cas où la police de Nice (dont lui) étaient ceux qui maitrisaient le mieux le sujet et que l'OCLCTIC était en dessous. Et que pendant longtemps il y a eu dénégation. Aujourd'hui, l'OCLCTIC dit que Nice a le meilleur niveau.
De ce point de vue-là, PP dit préférer la mentalité des gendarmes. Notamment car ils savent recruter à l'extérieur de la gendarmerie, des ingénieurs, etc. Ce que la police ne fait que sur concours. « *On ne recrute pas des talents.* » D'ailleurs, la gendarmerie était plus encline à travailler avec Florent Curtet que la police.
Il cite Jean-Marc Boget, patron du Comcybergend [sur le départ en juillet 2023]

**Les hackers éthiques et leur communauté**

Il parle d'une vraie communauté de hackers éthiques en France. Qui revendique une « pureté originelle » (sic), c'est-à-dire qui n'a jamais commis de péchés, verser dans l'illégal. Donc des profils comme FC sont gris et sont à la lisière de cette communauté.
Et cette communauté n'est pas celle des experts cybersécurité classiques (défenseurs/blue teamers). Ils utilisent l'offensif.
Toutefois, ils n'utilisent/maitrisent pas les techniques les plus poussées et de très haut niveau en hacking/pénétration. Car justement, ils ne sont pas dans la cybercriminalité, qui vise la plus grande efficacité avec un travail acharné à élaborer des armes numériques, à percer les défenses pour des raisons lucratives.

La communauté des hackers éthiques sont souvent des red teamers. On ne peut pas être les deux / à la fois : blue teamer et red teamer à la fois, attaquant et défenseur. Et même si on n'est pas black hat, on va acheter des outils criminels pour les étudier (rétro-inéginierie) et les maitriser. Exemple, le malware Zeus (cheval de Troie). Zeus à l'origine est développé par des hackers biélorusses, il a été diffusé, modifié/ « upgradé » par des Russes pour en faire un outil encore plus puissant.
On ne peut pas être un bon hacker éthique si on ne se frotte pas à ces outils.
Ça pose la question de la CTI. A ma question, il répond qu'il ne sait pas mais pense que la CTI (surtout en boite privée, donc l'équivalent du RIC dans le renseignement d'Etat) va chercher ces outils également.

Aujourd'hui les meilleurs attaquants sont la Chine, les USA et la Russie selon lui.

**Que pense-t-il du campus cyber ?**

Probablement un minimum de synergie selon lui, avec un peu de compétence, mais globalement surtout une opération de communication et immobilière.
« *C'est dommage qu'on ne sache pas travailler avec des cyberhackers français.* »

« C'est ce qu'essaie de proposer Hackers without Borders. Ça va prendre du temps. »
Le pouvoir est trop centralisé en France. Pourquoi ce projet de campus à Paris ?

« *Par contre on travaille au campus avec des entreprises, mais le comble c'est qu'il y a - beaucoup - des boîtes américaines qui n'ont rien à faire là !* »
Il évoque également les « promoteurs » venant des USA et qui infiltrent toute la communication autour du campus cyber et vendent des solutions américaines. « *Ils ont es compétences, mais ils n'ont rien à faire là !* »

**Cas belge et allemand**

En Belgique, libéralisation de l'approche bug bounty confirme-t-il. Pourquoi cette mentalité différente de celle de la France, même si c'est récent. Plus petit pays, plus facile à gérer se questionne-t-il ? Il n'est pas trop pour en France. Selon lui, bien sûr il y aurait un effet pervers. On est « choqué » ici de cette approche belge parce qu'on a peur que des failles soient découvertes par des « méchants ». Il vaut mieux un encadrement.

Le cas du CCC allemand. Il dit que ça n'a pas été toujours rose, mais que oui c'est positif et loin de ce qu'on a en France. Au début, ils avaient alerté en piratant une banque allemande et il y avait eu frictions. Ensuite, ils ont réussi à s'imposer comme une interface qui discute avec l'Etat.

**Rapport hackers-entreprises**

« *Ça commence à rentrer dans les mœurs. Mais c'est une très très lente prise de conscience* (sic). »

« On n'est pas des cibles » disent-elles en général. Le cas de Voyageurs du monde et du hacking de milliers de passeports à la suite de la fuite/attaque est significative.
PP montre son mécontentement et dit qu'il faudrait punir ce genre de patron : « *C'est ça qui devrait être puni. Ça devrait être puni, c'est irresponsable.* ». En effet, celui-ci a dit que ce n'était pas grave, « que c'était seulement 1% de nos passeports. »
Selon PP, ça montre la méconnaissance totale du milieu criminel, une désinvolture manifeste quant aux données personnelles et l'impact que peut avoir leur revente à des fins criminelles.

On n'a pas encore les bons réflexes en France pour beaucoup d'entreprises.

Même les plus sérieuses subissent les chocs. Et de citer le cas Virbac, dont la communication a été mesurée et responsable. Ils ont remonté les failles, pas du tout comme Voyageurs du monde dit-il, qui ont simplement restauré les données sans chercher comment les pirates étaient entrés.
Virbac a été réactive. L'ironie, c'est que leur RSSI, qui est très sérieux et reconnu (il organise des CTFs), avait initié une mission de pentesting avec blue/red teams juste avant l'attaque.
C'est une bonne démarche dit PP.

# BIBLIOGRAPHIE / SITOGRAPHIE

## A. Bibliographie alphabétique


ALLOING Camille, « La sousveillance. Vers un renseignement ordinaire », *in* « Le renseignement, un monde fermé dans une société ouverte », *Hermès*, 2016/3 (n°76), pp. 68-73.

ARPAGIAN Nicolas, *La cybersécurité*, « Que sais-je ? », PUF, 2022.

ARQUILLA John & RONFELDT David, *The Emergence of Noopolitik: Toward an American Information Strategy*, RAND corporation, 1999.

ASSENS Christophe & PERRIN Christelle, « L'intelligence économique : une stratégie de réseau pour les entreprises », *Revue internationale d'intelligence économique*, 2011/2 (Vol. 3), pp. 137-151.

AUDINET Maxime et MARANGÉ Céline, « La Russie : "l'espace informationnel" comme terrain de conflictualité », *Les guerres de l'information à l'ère numérique*, PUF, 2021, pp. 115-136.

BARTLETT Jamie, *The Dark Net: Inside the Digital Underworld*, Melville House, 2016.

BAUD Jacques, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002.

BAUMARD Philippe, *Le vide stratégique*, CNRS, 2012.

BAZZELL Michael, *OSINT Techniques: Resources for Uncovering Online Information*, Tenth, 2023.

BEAU Francis, *Le renseignement au prisme des sciences de l'information*, thèse de doctorat en sciences de l'information et de la communication, université de Valenciennes, 2019.

BEAUVOIS Jean-Léon & JOULE Robert-Vincent, *Petit traité de manipulation à l'usage des honnêtes gens*, PUG, 2014.

BEIRNAERT-HUVELLE Jacques, DUBOURGNOUX Rémi, CLARHAUT Joffrey, EBEL Franck, *Sécurité informatique – Ethical Hacking : Apprendre l'attaque pour mieux se défendre* (6e éd.), Éd. ENI, 2022.

BENEDICT Kevin, *Enterprise Mobility, Netcentric Operations and Military Mobility*, 24 août 2011 (https://mobileenterprisestrategies.blogspot.com/2011/08/enterprise-mobility-netcentric.html)

BERGÉ Jean-Sylvestre & GRUMBACH Stéphane, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », *Journal du droit international*, Clunet, n°4, Octobre 2016, var. 6.

BERGÈRE Sylvain, *Une contre-histoire de l'internet*, film documentaire, *Premières lignes Télévision/OWNI*, 2013, 86mn.

BERTRAN Marie-Gabrielle, « La place des logiciels libres et open source dans les nouvelles politiques du numérique en Russie », *Hérodote*, 2020, pp. 235-252

BLANC Sabine & NOOR Ophélia, *Hackers : Bâtisseurs depuis 1959*, OWNI, 2012.

BLOCH Laurent, *Communication de conflictualité et mouvements activistes sur Internet (2006-2011)*, thèse de doctorat en sciences de l'information et de la communication, université de Paris II – Panthéon Assas, 2016.

BONIFACE Pascal, *La volonté d'impuissance. La fin des ambitions internationales et stratégiques ?,* Seuil, 1996.

BORN Matteo, *Hackers : l'intimité violée*, film documentaire, Arte, 2023.

BORTZMEYER Stéphane, *Cyberstructure : L'Internet, un espace politique*, C&F Editions, 2018.

BOULANGER Philippe, *Planète médias. Géopolitique des réseaux et de l'influence*, Armand Colin, 2021.

BOURRET Christian, « Pistes de réflexions sur les actions et les potentialités de la Gendarmerie nationale. Le cas du Couserans dans le département de l'Ariège (Pyrénées) », *Cahiers de la sécurité et de la justice*, 2022/3 (n°56), pp. 44-51.

BOYD John R., *Destruction and Creation*, USCGSC, KS, 1976.

BOYER Bertrand, *Cyberguérilla 2.0*, École de guerre éditions, 2021.

BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, Nuvis, 2014.

BOYER Bertrand, *Cyberstratégie. L'art de la guerre numérique*, Nuvis, 2012.

BROOKING Emerson T. & SINGER Peter W., *LikeWar: The Weaponization of Social Media*, HMH Books, 2018.

BULINGE Franck et MOINET Nicolas (dir.), « Le renseignement, un monde fermé dans une société ouverte », *Hermès*, 2016/3 (n°76).

BULINGE Franck, MOINET Nicolas, « L'intelligence économique : un concept, quatre courants », *Sécurité et stratégie*, 2013/1 (12), pp. 56-64.

BULINGE Franck, *De l'espionnage au renseignement. La France à l'âge de l'information*, Vuibert, 2012.

CARAYON Bernard, *Patriotisme économique, de la guerre à la paix économique*, Le Rocher, 2006.

CARAYON Bernard, *Intelligence économique, compétitivité et cohésion sociale*, rapport au Premier ministre, juillet 2003.

CARCANO Andrea, DRAGONI Younes, KROTOFIL Marina, How TRITON Disrupted Safety Systems & Changed the Threat Landscape of Industrial Control Systems, conférence Black Hat USA 2018.

CARLESON J.C., *Work Like a Spy: Business Tips from a Former CIA Officer*, Portfolio, 2013.

CASTELLS Manuel, *La société en réseaux – T1 : L'ère de l'information*, Fayard, 1998.

CATTARUZZA Amaël & LIMONIER Kevin, « Le cyberespace, nouveau lieu de conflictualités géopolitiques », *Introduction à la géopolitique* Armand Colin, 2019.

CCDCOE (NATO), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.

CHARON Paul & JEANGENE VILMER Jean-Baptiste, *Les opérations d'influence chinoises. Un moment machiavélien*, IRSEM, 2021.

CHAUVANCY Raphaël, *Les nouveaux visages de la guerre*, VA, 2023.

CHIGNARD Simon et BENYAYER Louis-David, *Datanomics. Les nouveaux business models des données*, FYP, 2015.

CHOPIN Olivier & OUDET Benjamin, *Renseignement et sécurité*, Armand Colin, 2019.

CIALDINI Robert, *Influence et manipulation. L'art de la persuasion*, Pocket, 2014.

COLON David, *La guerre de l'information : Les États à la conquête de nos esprits*, Tallandier, 2023.

COLEMAN Gabriella, *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, 2013.

COUSSI Olivier, KNAUF Audrey, MOINET Nicolas, « Les guerres pour, par et contre l'information », *Revue internationale d'intelligence économique*, 2021/1 (Vol. 13), 184 p.

COUSSI Olivier, MOINET Nicolas, « Extension du domaine de la prédation. La vente d'Alstom à General Electric », *Revue française de gestion*, 2019/8 (n°285), pp. 211-227.

CURIEN Nicolas, « Inventer ensemble notre futur numérique : une ardente obligation ! », *Prospective et Stratégie*, n°9, 2018/1, pp. 23-35.

CURTET Florent (avec Sophie Garcin), *Hacke-moi si tu peux. Mémoires d'un cyperpirate repenti*, Le cherche midi, 2023.

DACHEUX Éric (dir.), *Les sciences de l'information et de la communication*, CNRS Éditions, 2009.

DAVENPORT Tara, « Cyber Attacks Against Submarine Cables: Gaps in International Law », *Submarine Networks World*, Center for International Law, National University of Singapore, 2018.

DEBLIQUY Pierre-Yves, *Chercher n'est pas trouver*, Édipro, 2014.

DE COLNET Augustin, *Compétition mondiale et intelligence économique*, VA, 2021.

DELBECQUE Éric, *L'intelligence économique : une nouvelle culture pour un nouveau monde*, PUF, 2006.

DE MAISON ROUGE OLIVIER, DELBECQUE Éric, LAÏDI Ali, HARBULOT Christian, « Penser la guerre économique », conférence tenue à l'IEP de Lyon, 29 novembre 2018.

DE MONTCHRESTIEN Antoine, *Traicté de l'oeconomie politique : dédié en 1615 au Roy et à la Reyne mère du Roy (Éd. 1889)*, Hachette-BNF, 2012.

DE MONTBRIAL Thierry, « La guerre économique mondiale, critique de T. de Montbrial », *Revue des deux mondes*, 1992, pp. 125-132.

DESARNAUD Gabrielle, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Études de l'Ifri*, janvier 2017.

DESCHAMPS Christophe & MOINET Nicolas*, La boîte à outils de l'intelligence économique*, Dunod, 2017.

DESCHAUX-DUTARD Delphine (dir.), « Cybersécurité internationale », *Introduction à la sécurité internationale*, PUG, 2018, pp. 209-225.

DESFORGES Alix, « Souveraineté numérique en France : du débat polarisé aux actes dispersés », *La Cyberdéfense. Politique de l'espace numérique*, 2023, pp. 127-133.

DESFORGES Alix, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques » *in* "Géopolitique de la datasphère", *Hérodote*, 2020, pp. 179-195.

DESFORGES Alix, *Approche géopolitique du cyberespace : les enjeux pour la défense et la sécurité nationale : l'exemple de la France*, thèse de Doctorat en géopolitique, université Paris 8, 2018.

DESFORGES Alix, « Les représentations du cyberespace : un outil géopolitique », *in* "Cyberespace : enjeux géopolitique", *Hérodote*, 2014/1-2 (n°152-153), pp. 67-81.

DOSSÉ Stéphane & KEMPF Olivier (dir.), « Les principes stratégiques du milieu cyber », *in* "Stratégies dans le cyberespace", *Cahiers de l'alliance géostratégique* (n°2), L'esprit du livre, 2011, pp. 181-188.

DOTAN Shimon & FERGUSON Charles, *Cybermonde. Le monde d'aujourd'hui*, film documentaire, Arte, États-Unis, 2023.

DOUZET Frédérick (dir.), « Géopolitique de la datasphère. Enjeux stratégiques de la révolution numérique », *Hérodote* 2020/2-3 (n°177-178), 2020.

DOUZET Frédérick, « Le Cyberespace. un enjeu de géopolitique majeur », *Le Monde*, 22-23/07/2018.

DOUZET Frédérick (dir.), « Cyberespace : enjeux géopolitiques », *Hérodote* n°152-153, 2014.

DUFOURCQ Jean, « L'influence comme 6e fonction stratégique », *Revue Défense Nationale*, 2023/1 (n°856), pp. 49-52.

DUMAS Philippe, *Information et action*, HDR, université du Sud Toulon-Var, 1991.

DYLEWSKI Philippe, *Le Renseignement Offensif : 300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs*, Agakure, 2021.

ELAZARI Keren, *Conférence TED*, 10 juin 2014.

ÉSAMBERT Bernard, *La Guerre économique mondiale*, Olivier Orban, 1991.

ÉSAMBERT Bernard, *Le Troisième Conflit mondial*, Plon, 1977.

FANTINO Benoit, *Quels éléments d'influence pour l'adoption symbolique de la sécurité des systèmes d'information ?*, thèse de doctorat en sciences de gestion, université d'Aix-Marseille, 2018.

FRIEDMAN Allan & SINGER Peter W., *Cybersecurity and Cyberwar: What Everyone Needs to Know®*, Oxford University Press, 2014.

FOGG, Brian J., *Persuasive technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, 2003.

FOUCAULT Michel, *Surveiller et punir. La naissance de la prison*, Gallimard, 1975.

FRANCIS Fanch, *De la prédiction à la détection d'évènements : L'analyse des mégadonnées au service du renseignement de sources ouvertes*, thèse de doctorat en sciences de l'information et de la communication, université de Lille, 2019.

FRANÇOIS Ludovic et ZERBIB Romain (dir.), *Influentia : la référence des stratégies d'influence*, Lavauzelle, 2015.

FRANÇOIS Ludovic, « La question éthique dans la pratique de l'intelligence économique », *Sécurité et stratégie*, 2010/HS1 (3), pp. 43-52.

GAGLIANO Giuseppe, *Guerre et intelligence économique dans la pensée de Christian Harbulot*, VA, 2016.

GALEOTTI Mark, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 2022.

GAUTIER Louis, « Cyber : les enjeux pour la défense et la sécurité des Français », *Politique étrangère*, 2018, pp. 29-42.

GENELOT Dominique, *Manager dans la complexité. Réflexions à l'attention des dirigeants*, INSEP Éditions, 2011.

GERGORIN Jean-Louis & ISAAC-DOGNIN Léo, *Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?*, Institut Diderot, juillet 2022.

GERGORIN Jean-Louis & ISAAC-DOGNIN Léo, *Cyber. La guerre permanente*, Les éditions du Cerf, 2018.

GERY Aude, « La stratégie française de cyberdéfense », *Brennus 4.0. Lettre d'information du CDEC*, mars 2020.

GIBSON William, *Neuromancien*, La Découverte, 1985.

GILPIN Robert, *The Political Economy of International Relations*, Princeton University Press, 1987.

GIOE David, STEVENS Tim, GOODMAN Michael S., « Intelligence in Cyber Era: Evolution or Revolution? » *Political Science Quarterly*, 2020, pp. 191-224.

GLADWELL Malcolm, *Le Point de bascule. Comment faire une grande différence avec de très petites choses*, Flammarion, 2016.

GORIA Stéphane, « L'utilité de l'échelle opératique pour considérer des stratégies d'intelligence et de guerre économique », *Revue internationale d'intelligence économique*, 2021/2 (Vol. 13), pp. 43-60.

GROVE Andy, *Seuls les paranoïaques survivent*, Village mondial, 1997.

GUIBERT Isabelle & JEANNIN Frédéric, *Les nouvelles frontières numériques. RGPD et politiques de protection des données*, VA, 2019.

GUILHON Alice & MOINET Nicolas (dir.), *Intelligence économique. S'informer, se protéger, influencer*, Eyrolles, 2016.

GUITON Amaëlle, *Hackers, au cœur de la résistance numérique*, Diable Vauvert, 2013.

GUYAUX Jean (général), *L'espion des sciences*, Flammarion, 2002.

HALLÉE, Yves & GARNEAU, Julie M. É., « L'abduction comme mode d'inférence et méthode de recherche : de l'origine à aujourd'hui », *Recherches qualitatives*, 38(1), 2019, pp. 124–140.

HARBULOT Christian, MOINET Nicolas, DE MORGNY Arnaud (dir.), *Guerre économique : comment gagner ?*, Nouveau Monde Éditions, 2023.

HARBULOT Christian, LAURENT Lucie, MOINET Nicolas, *Guerre économique : qui est l'ennemi ?*, Nouveau Monde Éditions, 2022.

HARBULOT Christian (entretien avec), « Chine/Etats-Unis ? Sortie de crise ?... La guerre économique systémique comme grille de décryptage » *Communication & Influence*, n°111, mai 2020.

HARBULOT Christian, *L'art de la guerre économique. Surveiller, analyser, protéger, influencer*, VA, 2018.

HARBULOT Christian, *Techniques offensives et guerre économique*, La Bourdonnaye, 2014.

HEATON Janet, *Reworking Qualitative Data*, Sage Publications, 2004.

HENROTIN Joseph, « Cyberdéfense : une généalogie », *La Cyberdéfense. Politique de l'espace numérique*, 2023, pp. 115-122.

HIMANEN Pekka, *L'éthique hacker et l'esprit de l'ère de l'information*, Exils, 2001.

HOLEINDRE Jean-Vincent (dir.), *La ruse et la force. Une autre histoire de la stratégie*, Perrin, 2017.

HUYGHE François-Bernard, KEMPF Olivier, MAZZUCCHI Nicolas, *Gagner les cyberconflits. Au-delà du technique*, Economica, 2015.

HUYGHE François-Bernard, « Les nouveaux jeux de l'influence », in *Business sous influence*, Éditions d'Organisation, 2004.

JAVERS Eamon, *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage*, Harper Business, 2010.

JORDANOV Alex, *Les guerres de l'ombre de la DGSI - Plongée au cœur des services secrets français*, Nouveaux mondes Éditions, 2019.

KEMPF Olivier, *Introduction à la cyberstratégie*, Economica, 2012.

KEMPF Olivier & DOSSÉ Stéphane (dir.), « Stratégies dans le cyberespace », *Cahiers de l'alliance géostratégique* (n°2), L'esprit du livre, 2011, pp. 181-188.

KLEIN Naomi, *No Logo : La tyrannie des marques*, Babel, 2002.

KNAPPENBERGER Brian, *The Internet's Own Boy: The Story of Aaron Swartz*, film documentaire, 2014, 1h45.

KUHN Thomas S., *La Structure des révolutions scientifiques*, Flammarion, 1992 (rééd. 2008).

LACOSTE Pierre, « Quel renseignement pour le XXIe siècle ? », *Actes du colloque au Carré des Sciences du 3 avril 2001*, Panazol, Éditions Lavauzelle, 2021.

LACOSTE Pierre & THUAL François, *Services secrets et géopolitique*, Lavauzelle, 2001.

LACOSTE Yves, *La géographie, ça sert, d'abord, à faire la guerre*, La Découverte Poche, 2014.

LACOSTE Yves, *Dictionnaire de géopolitique*, Flammarion, 1996.

LAÏDI Ali, *Le Droit, nouvelle arme de guerre économique : Comment les États-Unis déstabilisent les entreprises européennes*, Babel, 2020.

LAÏDI Ali, *Histoire mondiale de la guerre économique*, Perrin, 2016.

LALLEMENT Michel, *L'Âge du faire. Hacking, travail, anarchie*, Point, 2018.

LE DEZ Arnaud, *Tactique cyber. Le combat numérique*, Economica, 2019.

LEGAVRE Jean-Baptiste et RIEFFEL Rémy, *Les 100 mots des sciences de l'information et de la communication*, « Que sais-je ? », PUF, 2017.

LEVY Steven, *Hackers: Heroes of the Computer Revolution*, Doubleday, 1984 ; *L'Éthique des hackers*, Globe, 2013 (trad.).

LIBAERT Thierry & MOINET Nicolas, « La communication, clé de voûte de l'intelligence économique », *Communication et organisation*, n°42, 2012, pp. 5-10.

LICKLIDER Joseph C. R. & TAYLOR Robert, « The computer as a communication device », *Science and Technology*, avril 1968.

LIENARD Alexandre, *L'art (secret) de la guerre : essai sur la défense numérique. Le manuel de guerre du CISO*, Les Éditions de l'ASPIC, 2022.

LIENEMANN Marie-Noëlle, LEMOYNE Jean-Baptiste, PRIMAS Sophie, *Anticiper, adapter, influencer : l'intelligence économique comme outil de reconquête de notre souveraineté*, Rapport d'information au Sénat, juillet 2023.

LIMONIER Kevin, & AUDINET Maxime (dir.), « OSINT, enquêtes et terrains numériques », *Hérodote* (n°186), La découverte, 2022.

LOHARD Audrey, « La genèse inattendue du cyberespace de William Gibson », *in* "Cyberesp@ce & territoires", *Quaderni*, n°66, 2008, pp. 11-13.

LONG Johnny, *Google Hacking. Mettez vos données sensibles à l'abri des moteurs de recherches,* Dunod, 2005.

LOROT Pascal, « De la géopolitique à la géoéconomie », *Géoéconomie*, 2009/3 (n°50), pp. 9-19.

LOROT Pascal & THUAL François, « La géoéconomie, nouvelle grammaire des rivalités internationales », *Introduction à la géopolitique*, Montchrestien, 2002.

LOROT Pascal, *Introduction à la géoéconomie*, Economica, 1999.

LUTTWAK Edward, « L'arsenal de la géoéconomie », *Revue des deux mondes*, avril 1995.

LUTTWAK Edward, *Le rêve américain en danger*, Odile Jacob, 1995.

LUTTWAK Edward, "From Geopolitics to Geo-economics. Logics of Conflict, Grammar of Commerce", *The National Interest*, été 1990.

MARANGÉ Céline & QUESSARD Maud, *Les guerres de l'information à l'ère numérique*, PUF, 2021.

MARCON Christian & MOINET Nicolas, *Stratégie réseaux. Essai de stratégie*, ZéroHeure, 2000.

MARTIN (LTC), *OSINT : L'Art de collecter l'information ouverte*, Éd. du Château, 2023.

MARTIN Olivier, « Le mythe du "pouvoir égalisateur du cyber" », *Revue Défense Nationale*, 2019/8 (n°823), pp. 71-75.

MARTRE Henri, CLERC Philippe, HARBULOT Christian, *Rapport du groupe « Intelligence économique et stratégie des entreprises »*, 1994.

MASSÉ Guy & MOINET Nicolas, *Petit bréviaire contre l'intelligence superficielle*, VA, 2021.

MASSÉ Guy & THIBAULT Françoise, *Intelligence économique : un guide pour une économie de l'intelligence*, Bruxelles, De Boeck, 2001.

MATTELART Armand, *Histoire de la société de l'information*, La Découverte, (5e éd.), 2018.

MATTELART Armand, *La mondialisation de la communication*, PUF – Que sais-je ?, 1996, pp. 3-4.

MATTATIA Fabrice, « Faut-il dépénaliser les hackers blancs ? », *Revue de science criminelle et de droit pénal comparé*, 2015/4 (n° 4), pp. 837-846.

MAZZUCCHI Nicolas, « La cyberconflictualité et ses évolutions, effets physiques, effets symboliques », *Revue Défense Nationale*, 2019/6 (N° 821), pp. 138-143.

MITNICK Kevin D. & SIMON William L., *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2003.

MOINET Nicolas, *Les sentiers de la guerre économique*. T2 – *"Soft Powers"*, VA, 2020.

MOINET Nicolas, « Le renseignement au prisme du couple agilité-paralysie », *Prospective et stratégie*, 2019/1 (n°10), pp. 13-27.

MOINET Nicolas, *Les sentiers de la guerre économique*. T1 – *L'école des nouveaux "espions"*, VA, 2018.

MOINET Nicolas, « La communication, dimension oubliée de l'intelligence économique », *Communication & Organisation*, PUB, 2012/2 (n°42).

MOINET Nicolas, *Petite histoire de l'intelligence économique. Une innovation "à la française"*, L'Harmattan, 2010.

MOINET Nicolas, « De l'information utile à la connaissance stratégique : la dimension communicationnelle de l'intelligence économique », *Communication & Organisation*, n°35, décembre 2009, pp. 214-225.

MOINET Nicolas, « L'agilité stratégique : une question de dispositif intelligent », *Vie & sciences de l'entreprise*, 2007/1-2 (n°174-175), pp. 142-155.

MOINET Nicolas, *Dispositifs intelligents et stratégies d'innovation : la dimension stratégique de l'information et de la communication dans les réseaux de la recherche-développement*, thèse de doctorat en sciences de l'information et de la communication, université de Poitiers, 1999.

MOREL Camille, *Les câbles sous-marins*, Biblis, 2023.

MOREL Camille, *L'État et le réseau mondial de câbles sous-marins de communication*, thèse de doctorat en droit public, université de Lyon 3, 2020.

MORIN Edgard, *Les Sept savoirs nécessaires à l'éducation du futur*, Points, 2015.

MORIN Edgard, *Introduction à la pensée complexe*, Points, 2014.

MORIN Edgard, *La Méthode*, T.1 & T.2, Seuil, 2008.

MOSCAROLA Jean, *Faire parler les données. Méthodologie quantitatives et qualitatives*, EMS Éditions, 2018.

MUCCHIELLI Alex, « Pour des recherches en communication », in "La recherche en communication", *Communication & organisation*, ISIC-GRECO/O, n°10, 1996.

NASIR-BABA Ahmed, *Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience*, thèse de doctorat en sciences informatiques et cybersécurité, Institut des Mines-Télécom (IMT) d'Alès, université de Nîmes, 2022.

NIETO GOMEZ Rodrigo, « Cybergéopolitique : de l'utilité des cybermenaces », *in* "Cyberespace : enjeux géopolitiques", *Hérodote*, 2014, pp. 98-122.

NOCETTI Julien, « Des acteurs systémiques ? Les GAFAM au centre des jeux internationaux », in *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2023, pp. 174-181.

NOCETTI Julien, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018/2, pp. 15-27.

NODINOT Laurent & ELHIAS Marc (alias Christian Harbulot), *Il nous faut des espions ! Le Renseignement occidental en crise*, Robert Laffont, 1988.

NUÑEZ MOSCOSO Javier, « Et si l'on osait une épistémologie de la découverte ? La démarche abductive au service de l'analyse du travail enseignant », *Penser l'éducation*, 33, 2013, pp. 57-80.

PAQUIN Stéphane, *Économie politique internationale*, Paris, Montchrestien, 2009.

PATINO Bruno, *La civilisation du poisson rouge : Petit traité sur le marché de l'attention*, Grasset, 2019.

PECH Yannick, « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », *Prospective et stratégie*, 2019/1 (n°10), pp. 73-102.

PECH Yannick, *L'influence du renseignement dans la formulation de la politique étrangère depuis 1991. Approche comparée de l'impact des cultures du renseignement américaine et française sur le processus décisionnel*, mémoire de M2 en science politique-Relations internationales, université de Lyon 3, 2013.

PENALBA Pierre, *Darknet, le voyage qui fait peur. Du fantasme à la réalité*, Albin Michel, 2022.

PERAYA Daniel, *in* « Le dispositif. Entre usage et concept », *Hermès*, 1999/3 (n°25), pp. 153-167.

PINARD Maxime, « L'hacktivisme dans le cyberespace : quelles réalités ? », *Revue internationale et stratégique*, 2012/3 (n°87), pp. 93-101.

PITRON Guillaume, *L'enfer numérique : voyage au bout d'un like*, Les liens qui libèrent, 2021.

PROCTOR Robert N., *Agnotology: The Making and Unmaking of Ignorance*, 1st, 2008.

« RED TEAM », *Ces guerres qui nous attendent : 2030-2060*, Des Équateurs, 2022.

QIAO Liang & WANG Xiangsui, *La guerre hors limites*, Payot & Rivages Éd., 2006.

RICHARDSON Christopher, *Bridging the air gap: an information assurance perspective*, thèse de doctorat en science physique et ingénierie, université de Southampton, 2012.

RIETHMÜLLER Carolin, *Cybercriminalité, des attaques bien réelles*, film documentaire, Arte, Allemagne, 2023.

RUSS Jacqueline, *Les théories du pouvoir*, Le livre de poche, 1994, 349 p.

SAMUEL Alexandra W., *Hacktivism and the future of political participation*, Université de Harvard, 2004.

SCHNEIER Bruce, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company, 2018.

SCHWARTAU Winn, *Terminal Compromise: The First Cyberterrorism Attack on the U.S.*, Interpact Pr, 2020.

SEJEAN Marc, Intervention dans le cadre de la Conférence *CyberNeTic* du 27 avril 2023, IUT Bordeaux-Montaigne.

SHENK David, *Data Smog: Surviving the Information Glut*, HarperOne, 1997.

SNOWDEN Edward, *Mémoire vives*, Seuil, 2019.

SOUTOU Georges-Henri (dir.), « Stratégie du cyberespace Stratégique », *Stratégique*, Institut de Stratégie Comparée, 2017/4 (n°117).

SOUTOU Georges Henri, *La guerre froide*, Fayard, 2011.

SOUTOU Georges Henri, *Le sang et l'or. Les buts de guerre économiques des grandes puissances*, Fayard, 1990.

SPAFFORD, Eugene H., « James P. Anderson: An Information Security Pioneer », *IEEE Security & Privacy Magazine*, 2008, 6(1), p. 9–9.

STAMBOLIYSKA Rayna, *La face cachée d'internet*, Larousse, 2017.

STEELE Robert D., *On Intelligence: Spies and Secrecy in an Open World*, OSS International Press, 2016.

STOLL Clifford, *Le Nid du coucou. La longue traque d'un espion dans le labyrinthe de l'espionnage informatique*, Albin Michel, 1989.

STRANGE Susan, *Le retrait de l'État : la dispersion du pouvoir dans l'économie mondiale*, Temps présent, 2011.

TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Hérodote*, 2020/2-3 (n°177-178), pp. 313-328.

TALEB Nassim N., *Le cygne noir : La puissance de l'imprévisible*, Les Belles Lettres, 2008.

TISSEYRE Didier, « Le cyberespace, nouveau théâtre de conflits », *L'ENA hors les murs*, 2021/3 (n°504), pp. 40-42.

THOMAS Rid, « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n°1, 2011.

TRAIMOND Bernard, *L'économie n'existe pas*, Le Bord de l'Eau, 2011.

TROUCHAUD Philippe, *La Cybersécurité face au défi de la confiance*, Odile Jacob, 2018.

VARELA Fernando, « Constructivisme et énaction », *École thématique CNRS*, ARCo, 2006.

VÉDRINE Hubert, *Et après ?*, Fayard, 2020.

VERLEY Samuel & PERROTIN Élodie, *Qui sont les hackers ?*, Éd. du Ricochet, 2018.

WARUSFEL Bertrand, « Les notions de défense et de sécurité en droit français », *Droit & Défense*, n°94/4, octobre 1994.

WIENER Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine*, Hermann & Cie & MIT Press, 1948.

WILENSKY Harold, *Organizational Intelligence Knowledge and Policy in Government and Industry*, Basic Books, 1967.

WOLTON Dominique, « Communication, incommunication et acommunication », in *Les incommunications*, *Hermès*, 2019/2 (n°84), pp. 200-205.

ZIMMER Terry, *Le renseignement humain à l'ère numérique*, VA, 2018.

ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, Zulma, 2022.

---

## B. Bibliographie et sitographie thématiques

### *INTERNET, CYBERESPACE & CYBERSÉCURITÉ*

ARPAGIAN Nicolas, *La cybersécurité*, « Que sais-je ? », PUF, 2022.

BERGÉ Jean-Sylvestre & GRUMBACH Stéphane, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », *Journal du droit international*, Clunet, n°4, Octobre 2016, var. 6.

BARTLETT Jamie, *The Dark Net: Inside the Digital Underworld*, Melville House, 2016.

BERTRAN Marie-Gabrielle, « La place des logiciels libres et open source dans les nouvelles politiques du numérique en Russie », *Hérodote*, 2020, pp. 235-252

BORN Matteo, *Hackers : l'intimité violée*, film documentaire, Arte, 2023.

BORTZMEYER Stéphane, *Cyberstructure : L'Internet, un espace politique*, C&F Editions, 2018.

CHIGNARD Simon & BENYAYER Louis-David, *Datanomics. Les nouveaux business models des données*, FYP, 2015.

CURIEN Nicolas, « Inventer ensemble notre futur numérique : une ardente obligation ! », *Prospective et Stratégie*, n°9, 2018/1, pp. 23-35.

DAVENPORT Tara, « Cyber Attacks Against Submarine Cables: Gaps in International Law », *Submarine Networks World*, Center for International Law, National University of Singapore, 2018.

DOSSÉ Stéphane & KEMPF Olivier (dir.), « Les principes stratégiques du milieu cyber », *in* "Stratégies dans le cyberespace", *Cahiers de l'alliance géostratégique* (n°2), L'esprit du livre, 2011, pp. 181-188.

DOTAN Shimon & FERGUSON Charles, *Cybermonde. Le monde d'aujourd'hui*, film documentaire, Arte, États-Unis, 2023.

DOUZET Frédérick, « Le Cyberespace. un enjeu de géopolitique majeur », *Le Monde*, 22-23/07/18.

FANTINO Benoit, *Quels éléments d'influence pour l'adoption symbolique de la sécurité des systèmes d'information ?*, thèse de doctorat en sciences de gestion, université d'Aix-Marseille, 2018.

FOGG, Brian J., *Persuasive technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, 2003.

FRAGA-LAMAS Paula, FERNÁNDEZ-CARAMÉS Tiago M., SUÁREZ-ALBELA Manuel, CASTEDO Luis, GONZÁLEZ-LÓPEZ Miguel, « A review on internet of things for defense and public safety », *Sensors*, 16(10), 2016.

GAUTIER Louis, « Cyber : les enjeux pour la défense et la sécurité des Français », *Politique étrangère*, 2018, pp. 29-42.

GUIBERT Isabelle & JEANNIN Frédéric, *Les nouvelles frontières numériques. RGPD et politiques de protection des données*, VA, 2019.

LICKLIDER Joseph C. R. & TAYLOR Robert, « The computer as a communication device », *Science and Technology*, avril 1968.

LIENARD Alexandre, *L'art (secret) de la guerre : essai sur la défense numérique. Le manuel de guerre du CISO*, Les Éditions de l'ASPIC, 2022.

LOHARD Audrey, « La genèse inattendue du cyberespace de William Gibson », *in* "Cyberesp@ce & territoires", *Quaderni*, n°66, 2008, pp. 11-13.

MATTATIA Fabrice, « Faut-il dépénaliser les hackers blancs ? », *Revue de science criminelle et de droit pénal comparé*, 2015/4 (n°4), pp. 837-846.

NASIR-BABA Ahmed, *Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience*, thèse de doctorat en sciences informatiques et cybersécurité, Institut des Mines-Télécom (IMT) d'Alès, université de Nîmes, 2022.

NOCETTI Julien, « Des acteurs systémiques ? Les GAFAM au centre des jeux internationaux », in *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2023, pp. 174-181.

PITRON Guillaume, *L'enfer numérique : voyage au bout d'un like*, Les liens qui libèrent, 2021.

RIETHMÜLLER Carolin, *Cybercriminalité, des attaques bien réelles*, film documentaire, Arte, Allemagne, 2023.

SEJEAN Marc, Intervention dans le cadre de la Conférence *CyberNeTic* du 27 avril 2023, IUT Bordeaux-Montaigne.

STAMBOLIYSKA Rayna, *La face cachée d'internet*, Larousse, 2017.

TROUCHAUD Philippe, *La Cybersécurité face au défi de la confiance*, Odile Jacob, 2018.

WIENER Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine*, Hermann & Cie & MIT Press, 1948.

## Sitographie

*Sources secondaires/articles de presse*

https://www.eff.org/cyberspace-independence

https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

https://www.marianne.net/monde/crypto-ag-l-entreprise-suisse-qui-permis-la-cia-d-espionner-120-pays-pendant-quarante-ans

https://www.silicon.fr/secnumedu-39-formations-labellisees-461724.html

https://www.silicon.fr/health-data-hub-microsoft-2025-464572.html

https://www.challenges.fr/economie/le-cloud-souverain-version-sarkozy-est-mort-et-enterre_667076

https://www.latribune.fr/technos-medias/internet/numerique-souverain-octave-klaba-et-la-caisse-des-depots-creent-synfonium-un-champion-europeen-qui-veut-d-emblee-croquer-qwant-958352.html

https://www.lesechos.fr/idees-debats/cercle/opinion-gaia-x-un-cloud-europeen-souverain-1976239

https://www.itpro.fr/eric-filiol-france-incapable-capitaliser-hackers-20026/

https://www.lemonde.fr/blog/bugbrother/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/

https://www.inria.fr/fr/quatre-algorithmes-certifies-NIST-menace-ordinateur-quantique

https://www.youtube.com/watch?app=desktop&v=1DJ3qTW51FA (interview V. Poucheret et Brice Augras, chaine *Thinkerview*, 2021)

https://www.sstic.org/

gfcyber.org/cybersecurity-challenges-of-the-ksa-past-present-and-future/

cyberguerre.numerama.com/10676-les-dirigeants-de-solarwinds-accusent-un-stagiaire-de-la-fuite-du-mot-de-passe-solarwinds123.html

cyberguerre.numerama.com/10516-laffaire-solarwinds-bien-plus-quun-simple-incident-despionnage-pour-la-maison-blanche.html

https://web.archive.org/web/20220817083321/https://oda-alexandre.com/cybersecurite

https://www.numerama.com/politique/28295-bluetouff-condamne-en-appel-pour-avoir-su-utiliser-google.html

https://info.haas-avocats.com/droit-digital/laffaire-bluetouff-la-consecration-du-vol-de-donnees-informatiques#_ftn2

https://www.nextinpact.com/article/18067/95165-affaire-bluetouff-cour-cassation-consacre-vol-fichiers-informatiques

https://www.blogdumoderateur.com/whatsapp-conversations-privees-indexees-google/

https://www.numerama.com/tech/607210-sur-google-on-trouve-en-un-clic-des-milliers-de-numeros-francais-lies-a-whatsapp.htm

https://www.nextinpact.com/article/45437/haurus-dgsi-aux-droits-defense-en-passant-par-darkweb

https://www.leparisien.fr/high-tech/qu-est-ce-que-le-teorem-le-telephone-chiffre-que-benalla-a-oublie-de-rendre-16-01-2019-7990023.php

https://www.rtl.fr/actu/politique/bientot-un-nouveau-telephone-securise-pour-emmanuel-macron-790020960

https://www.village-justice.com/articles/hacker-ethique-detecter-les-vulnerabilites-pour-prevenir-les-cyberattaques,46474.html

https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php

*Sources primaires*

https://www.ssi.gouv.fr/actualite/fic-2019-lanssi-appelle-a-un-engagement-collectif-pour-stabiliser-le-cyberespace/

https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ ; https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_dossier presse.pdf

https://www.ssi.gouv.fr/entreprise/glossaire/c/

https://csrc.nist.gov/glossary/term/cyberspace

https://csrc.nist.gov/glossary/term/cyberspace

https://www.senat.fr/basile/visio.do?id=qSEQ220700681&idtable=q397252|q417232&_c=%22parquet+national+cyber%22&rch=gs&de=20030909&au=20230909&rqg=drqscpt&dp=20+ans&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn

https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information#_Toc256000143

https://www.senat.fr/notice-rapport/2019/r19-007-1-notice.html

https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information#

https://www.senat.fr/rap/r22-831-1/r22-831-1_mono.html

https://www.ssi.gouv.fr/actualite/au-college-et-au-lycee-former-a-la-cybersecurite-par-le-jeu/

https://www.ssi.gouv.fr/administration/formations/cyberedu/

https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/

https://campuscyber.fr/

https://www.campuscyber-na.fr/

https://www.senat.fr/seances/s202306/s20230628/s20230628008.html

https://videos.senat.fr/video.4011095_649c1f7021980?timecode=10424340

https://www.ietf.org/rfc/rfc1392.txt

https://www.ietf.org/standards/rfcs/

https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/

https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-4-chambre-10-arret-du-5-fevrier-2014/

https://www.senat.fr/colloques/office_du_juge/office_du_juge9.html

https://www.legifrance.gouv.fr/juri/id/JURITEXT000030635061/

https://www.legifrance.gouv.fr/loda/id/LEGIARTI000029755281/2014-11-15#LEGIARTI000029755281

https://www.senat.fr/basile/visio.do?id=qSEQ220700681&idtable=q397252|q417232&_c=%22parquet+national+cyber%22&rch=gs&de=20030909&au=20230909&rqg=drqscpt&dp=20+ans&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn

https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000028345141

https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/souvnum/l15souvnum2021048_compte-rendu#

https://www.assemblee-nationale.fr/14/rapports/r3399.asp

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345220

https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203174

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555

https://www.ejustice.just.fgov.be/eli/loi/2022/11/28/2022042980/justel#LNK0013

https://www.lepoint.fr/politique/pour-un-ministere-du-numerique-a-la-hauteur-de-nos-enjeux-25-06-2020-2381752_20.php

https://www.consilium.europa.eu/fr/policies/eu-industrial-policy/eu-chips-industry/

## *GÉOPOLITIQUE, GÉOPOLITIQUE DU CYBERESPACE*

BOULANGER Philippe, *Planète médias. Géopolitique des réseaux et de l'influence*, Armand Colin, 2021.

CATTARUZZA Amaël & LIMONIER Kevin, « Le cyberespace, nouveau lieu de conflictualités géopolitiques », *Introduction à la géopolitique* Armand Colin, 2019.

DESCHAUX-DUTARD Delphine (dir.), « Cybersécurité internationale », *Introduction à la sécurité internationale*, PUG, 2018, pp. 209-225.

DESFORGES Alix, « Souveraineté numérique en France : du débat polarisé aux actes dispersés », *La Cyberdéfense. Politique de l'espace numérique*, 2023, pp. 127-133.

DESFORGES Alix, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques » *in* "Géopolitique de la datasphère", *Hérodote*, 2020, pp. 179-195.

DESFORGES Alix, *Approche géopolitique du cyberespace : les enjeux pour la défense et la sécurité nationale : l'exemple de la France*, thèse de Doctorat en géopolitique, université Paris 8, 2018.

DESFORGES Alix, « Les représentations du cyberespace : un outil géopolitique », *in* "Cyberespace : enjeux géopolitique", *Hérodote*, 2014/1-2 (n°152-153), pp. 67-81.

DOUZET Frédérick (dir.), « Cyberespace : enjeux géopolitiques », *Hérodote* n°152-153, 2014.

DOUZET Frédérick (dir.), « Géopolitique de la datasphère. Enjeux stratégiques de la révolution numérique », *Hérodote* 2020/2-3 (n°177-178), 2020.

LACOSTE Yves, *La géographie, ça sert, d'abord, à faire la guerre*, La Découverte Poche, 2014.

LACOSTE Yves, *Dictionnaire de géopolitique*, Flammarion, 1996.

MARTIN Olivier, « Le mythe du "pouvoir égalisateur du cyber" », *Revue Défense Nationale*, 2019/8 (n°823), pp. 71-75.

MOREL Camille, *Les câbles sous-marins*, Biblis, 2023.

MOREL Camille, *L'État et le réseau mondial de câbles sous-marins de communication*, thèse de doctorat en droit public, université de Lyon 3, 2020.

NIETO GOMEZ Rodrigo, « Cybergéopolitique : de l'utilité des cybermenaces », *in* "Cyberespace : enjeux géopolitiques", *Hérodote*, 2014, pp. 98-122.

VÉDRINE Hubert, *Et après ?*, Fayard, 2020.

## Sitographie

https://www.monde-diplomatique.fr/cartes/cables-sous-marins

## *CYBERGUERRE, CYBERDÉFENSE & CYBERSTRATÉGIE*

BENEDICT Kevin, *Enterprise Mobility, Netcentric Operations and Military Mobility*, 24 août 2011 (https://mobileenterprisestrategies.blogspot.com/2011/08/enterprise-mobility-netcentric.html)

BOYER Bertrand, *Cyberguérilla 2.0*, École de guerre éditions, 2021.

BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, Nuvis, 2014.

BOYER Bertrand, *Cyberstratégie. L'art de la guerre numérique*, Nuvis, 2012.

CARCANO Andrea, DRAGONI Younes, KROTOFIL Marina, *How TRITON Disrupted Safety Systems & Changed the Threat Landscape of Industrial Control Systems*, conférence Black Hat USA 2018.

CCDCOE (NATO), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.

DESARNAUD Gabrielle, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Études de l'Ifri*, janvier 2017.

DUFOURCQ Jean, « L'influence comme 6e fonction stratégique », *Revue Défense Nationale*, 2023/1 (n°856), pp. 49-52.

FRIEDMAN Allan & SINGER Peter W., *Cybersecurity and Cyberwar: What Everyone Needs to Know*®, Oxford University Press, 2014.

GERGORIN Jean-Louis & ISAAC-DOGNIN Léo, *Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?*, Institut Diderot, juillet 2022 (https://www.institutdiderot.fr/les-publications-de-linstitut-diderot/cyber-quelles-strategies-face-a-lexplosion-des-menaces/).

GERGORIN Jean-Louis & ISAAC-DOGNIN Léo, *Cyber. La guerre permanente*, Les éditions du Cerf, 2018.

GERY Aude, « La stratégie française de cyberdéfense », *Brennus 4.0. Lettre d'information du CDEC*, mars 2020.
(https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299)

GHAFFARIAN Seyed M. & SHAHRIARI Homayoun R., « Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey », *ACM Computing Surveys* (CSUR), 50(4), 2017, pp. 1-36.

HENROTIN Joseph, « Cyberdéfense : une généalogie », *La Cyberdéfense. Politique de l'espace numérique*, 2023, pp. 115-122.

HUYGHE François-Bernard, KEMPF Olivier, MAZZUCCHI Nicolas, *Gagner les cyberconflits. Au-delà du technique*, Economica, 2015.

KEMPF Olivier, *Introduction à la cyberstratégie*, Economica, 2012.

KEMPF Olivier & DOSSÉ Stéphane (dir.), « Stratégies dans le cyberespace », *Cahiers de l'alliance géostratégique* (n°2), L'esprit du livre, 2011, pp. 181-188.

LE DEZ Arnaud, *Tactique cyber. Le combat numérique*, Economica, 2019.

MAZZUCCHI Nicolas, « La cyberconflictualité et ses évolutions, effets physiques, effets symboliques », *Revue Défense Nationale*, 2019/6 (n°821), pp. 138-143.

NOCETTI Julien, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018/2, pp. 15-27.

« RED TEAM », *Ces guerres qui nous attendent : 2030-2060*, Des Équateurs, 2022. (https://www.defense.gouv.fr/aid/actualites/red-team-defense-devoile-ses-nouveaux-scenarii-menaces-conflictualites)

RICHARDSON Christopher, *Bridging the air gap: an information assurance perspective*, thèse de doctorat en science physique et ingénierie, université de Southampton, 2012.

SCHNEIER Bruce, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company, 2018.

SNOWDEN Edward, *Mémoire vives*, Seuil, 2019.

TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Hérodote*, 2020/2-3 (n°177-178), pp. 313-328.

TISSEYRE Didier, « Le cyberespace, nouveau théâtre de conflits », *L'ENA hors les murs*, 2021/3 (n°504), pp. 40-42.

THOMAS Rid, « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n°1, octobre 2011.

SOUTOU Georges-Henri (dir.), « Stratégie du cyberespace Stratégique », *Stratégique*, Institut de Stratégie Comparée, 2017/4 (n°117).

## Sitographie

*Sources secondaires/articles de recherche/articles de presse*

https://www.frstrategie.org/programmes/observatoire-armee-de-terre-2035/concept-russe-guerre-nouvelle-generation-general-gerasimov-quelle-exploitation-pour-armee-terre-2020

https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html

https://www.penseemiliterre.fr/fr/plugins/cdec/pdf/to_pdf.php?entry=114299

https://www.opex360.com/2022/11/09/m-macron-erige-linfluence-au-rang-de-fonction-strategique/

https://www.forbes.fr/technologie/ia-offensive-et-ia-defensive-les-defis-exponentiels-de-la-cybersecurite/

iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

https://technique-et-droit-du-numerique.fr/oiv-ose-critical-entities-projet-directive-ue-decembre-2020/

https://mobileenterprisestrategies.blogspot.com/2011/08/enterprise-mobility-netcentric.html

https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html

https://www.ifri.org/fr/publications/etudes-de-lifri/cyberattaques-systemes-energetiques-faire-face-risque

*Sources primaires*

https://www.c-dec.terre.defense.gouv.fr/images/multimedia/photo/une/20220114_champs-immateriels/20211125_NP_CDEC_PEP_Champs_immateriels_un_combat_de_l-information.pdf

https://www.c-dec.terre.defense.gouv.fr/images/documents/documents-doctrine/20210929_NP_CDEC_DDO_RFT_3-2-0-CEFT.pdf

https://archives.defense.gouv.fr/content/download/239576/2745135/Présentation_du_pacte Défense cyber.pdf

http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf

https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue_strategique_dsn_cle4b3beb.pdf

https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

https://www.senat.fr/rap/r11-681/r11-6811.pdf

https://www.defense.gouv.fr/dgris/politique-defense/livres-blancs

https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022

https://www.defense.gouv.fr/ema/chef-detat-major-armees/vision-strategique-du-chef-detat-major-armees-fresgb

https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def2021068_compte-rendu.pdf

http://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf

https://archives.defense.gouv.fr/portail/actualites2/florence-parly-presente-la-doctrine-militaire-de-lutte-informatique-d-influence.html

https://www.senat.fr/rap/r07-449/r07-449.html

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000634536

https://www.sgdsn.gouv.fr/publications/la-securite-des-activites-dimportance-vitale

https://www.senat.fr/rap/r22-638/r22-6385.html#toc37

https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline

## *INTELLIGENCE ÉCONOMIQUE & GUERRE SYSTÉMIQUE, GUERRE COGNITIVE & INFORMATIONNELLE*

ARQUILLA John & RONFELDT David, *The Emergence of Noopolitik: Toward an American Information Strategy*, RAND corporation, 1999.

ASSENS Christophe & PERRIN Christelle, « L'intelligence économique : une stratégie de réseau pour les entreprises », *Revue internationale d'intelligence économique*, 2011/2 (Vol. 3), pp. 137-151.

AUDINET Maxime & MARANGÉ Céline, « La Russie : "l'espace informationnel" comme terrain de conflictualité », *Les guerres de l'information à l'ère numérique*, PUF, 2021, pp. 115-136.

BAUMARD Philippe, *Le vide stratégique*, CNRS, 2012.

BEAUVOIS Jean-Léon & JOULE Robert-Vincent, *Petit traité de manipulation à l'usage des honnêtes gens*, PUG, 2014.

BLOCH Laurent, *Communication de conflictualité et mouvements activistes sur Internet (2006-2011)*, thèse de doctorat en sciences de l'information et de la communication, université de Paris II – Panthéon Assas, 2016.

BONIFACE Pascal, *La volonté d'impuissance. La fin des ambitions internationales et stratégiques ?,* Seuil, 1996.

BOURRET Christian, « Pistes de réflexions sur les actions et les potentialités de la Gendarmerie nationale. Le cas du Couserans dans le département de l'Ariège (Pyrénées) », *Cahiers de la sécurité et de la justice*, 2022/3 (n°56), pp. 44-51.

BOYD John R., *Destruction and Creation*, USCGSC, KS, 1976.

BROOKING Emerson T. & SINGER Peter W., *LikeWar: The Weaponization of Social Media*, HMH Books, 2018.

BULINGE Franck, MOINET Nicolas, « L'intelligence économique : un concept, quatre courants », *Sécurité et stratégie*, 2013/1 (12), pp. 56-64.

CARAYON Bernard, *Patriotisme économique, de la guerre à la paix économique*, Le Rocher, 2006.

CARAYON Bernard, *Intelligence économique, compétitivité et cohésion sociale*, rapport au Premier ministre, juillet 2003.

CASTELLS Manuel, *La société en réseaux – T1 : L'ère de l'information*, Fayard, 1998.

CHARON Paul & JEANGENE VILMER Jean-Baptiste, *Les opérations d'influence chinoises. Un moment machiavélien*, IRSEM, 2021.

CHAUVANCY Raphaël, *Les nouveaux visages de la guerre*, VA, 2023.

CIALDINI Robert, *Influence et manipulation. L'art de la persuasion*, Pocket, 2014.

COLON David, *La guerre de l'information : Les États à la conquête de nos esprits*, Tallandier, 2023.

COUSSI Olivier, KNAUF Audrey, MOINET Nicolas, « Les guerres pour, par et contre l'information », *Revue internationale d'intelligence économique*, 2021/1 (Vol. 13), 184 p.

COUSSI Olivier & MOINET Nicolas, « Extension du domaine de la prédation. La vente d'Alstom à General Electric », *Revue française de gestion*, 2019/8 (n°285), pp. 211-227.

DE COLNET Augustin, *Compétition mondiale et intelligence économique*, VA, 2021.

D'ELIA Danilo, « La guerre économique à l'ère du cyberespace », *Hérodote*, 2014/1-2 (n°152-153), pp. 240-260.

DE MAISON ROUGE OLIVIER, DELBECQUE Éric, LAÏDI Ali, HARBULOT Christian, « Penser la guerre économique », conférence tenue à l'IEP de Lyon, 29 novembre 2018.

DE MONTCHRESTIEN Antoine, *Traicté de l'oeconomie politique : dédié en 1615 au Roy et à la Reyne mère du Roy (Éd. 1889)*, Hachette-BNF, 2012.

DE MONTBRIAL Thierry, « La guerre économique mondiale, critique de T. de Montbrial », *Revue des deux mondes*, 1992, pp. 125-132.

DELBECQUE Éric, *L'intelligence économique : une nouvelle culture pour un nouveau monde*, PUF, 2006.

DESCHAMPS Christophe & MOINET Nicolas*, La boîte à outils de l'intelligence économique*, Dunod, 2017.

DUMAS Philippe, *Information et action*, HDR, université du Sud Toulon-Var, 1991.

ÉSAMBERT Bernard, *La Guerre économique mondiale*, Olivier Orban, 1991.

ÉSAMBERT Bernard, *Le Troisième Conflit mondial*, Plon, 1977.

FRAGA-LAMAS Paula, FERNÁNDEZ-CARAMÉS Tiago M., SUÁREZ-ALBELA Manuel, CASTEDO Luis, GONZÁLEZ-LÓPEZ Miguel, « A review on internet of things for defense and public safety », *Sensors*, 16(10), 2016.

FRANÇOIS Ludovic & ZERBIB Romain (dir.), *Influentia : la référence des stratégies d'influence*, Lavauzelle, 2015.

FRANÇOIS Ludovic, « La question éthique dans la pratique de l'intelligence économique », *Sécurité et stratégie*, 2010/HS1 (3), pp. 43-52.

GHAFFARIAN Seyed M. & SHAHRIARI Homayoun R., « Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey », *ACM Computing Surveys* (CSUR), 50(4), 2017, pp. 1-36.

GAGLIANO Giuseppe, *Guerre et intelligence économique dans la pensée de Christian Harbulot*, VA, 2016.

GALEOTTI Mark, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 2022.

GENELOT Dominique, *Manager dans la complexité. Réflexions à l'attention des dirigeants*, INSEP Éditions, 2011.

GILPIN Robert, *The Political Economy of International Relations*, Princeton University Press, 1987.

GLADWELL Malcolm, *Le Point de bascule. Comment faire une grande différence avec de très petites choses*, Flammarion, 2016.

GORIA Stéphane, « L'utilité de l'échelle opératique pour considérer des stratégies d'intelligence et de guerre économique », *Revue internationale d'intelligence économique*, 2021/2 (Vol. 13), pp. 43-60.

GROVE Andy, *Seuls les paranoïaques survivent*, Village mondial, 1997.

GUILHON Alice & MOINET Nicolas (dir.), *Intelligence économique. S'informer, se protéger, influencer*, Eyrolles, 2016.

HARBULOT Christian, MOINET Nicolas, DE MORGNY Arnaud (dir.), *Guerre économique : comment gagner ?*, Nouveau Monde Éditions, 2023.

HARBULOT Christian, LAURENT Lucie, MOINET Nicolas, *Guerre économique : qui est l'ennemi ?*, Nouveau monde, 2022.

HARBULOT Christian (entretien avec), « Chine/Etats-Unis ? Sortie de crise ?... La guerre économique systémique comme grille de décryptage » *Communication & Influence*, n°111, mai 2020.

HARBULOT Christian, *L'art de la guerre économique. Surveiller, analyser, protéger, influencer*, VA, 2018.

HARBULOT Christian, *Techniques offensives et guerre économique*, La Bourdonnaye, 2014.

HOLEINDRE Jean-Vincent (dir.), *La ruse et la force. Une autre histoire de la stratégie*, Perrin, 2017.

HUYGHE François-Bernard, « Les nouveaux jeux de l'influence », in *Business sous influence*, Éditions d'Organisation, 2004.

KLEIN Naomi, *No Logo : La tyrannie des marques*, Babel, 2002.

LAÏDI Ali, *Le Droit, nouvelle arme de guerre économique : Comment les États-Unis déstabilisent les entreprises européennes*, Babel, 2020.

LAÏDI Ali, *Histoire mondiale de la guerre économique*, Perrin, 2016.

LIBAERT Thierry & MOINET Nicolas, « La communication, clé de voûte de l'intelligence économique », *Communication et organisation*, n°42, 2012, pp. 5-10.

LIENEMANN Marie-Noëlle, LEMOYNE Jean-Baptiste, PRIMAS Sophie, *Anticiper, adapter, influencer : l'intelligence économique comme outil de reconquête de notre souveraineté*, Rapport d'information au Sénat, juillet 2023 (https://www.senat.fr/notice-rapport/2022/r22-872-notice.html).

LOROT Pascal, « De la géopolitique à la géoéconomie », *Géoéconomie*, 2009/3 (n°50), pp. 9-19.

LOROT Pascal & THUAL François, « La géoéconomie, nouvelle grammaire des rivalités internationales », *Introduction à la géopolitique*, Montchrestien, 2002.

LOROT Pascal, *Introduction à la géoéconomie*, Economica, 1999.

LUTTWAK Edward, « L'arsenal de la géoéconomie », *Revue des deux mondes*, avril 1995.

LUTTWAK Edward, *Le rêve américain en danger*, Odile Jacob, 1995.

LUTTWAK Edward, "From Geopolitics to Geo-economics. Logics of Conflict, Grammar of Commerce", *The National Interest*, été 1990.

MARANGÉ Céline & QUESSARD Maud, *Les guerres de l'information à l'ère numérique*, PUF, 2021.

MARCON Christian & MOINET Nicolas, *Stratégie réseaux. Essai de stratégie*, ZéroHeure, 2000.

MARTRE Henri, CLERC Philippe, HARBULOT Christian, *Rapport du groupe « Intelligence économique et stratégie des entreprises »*, 1994.

MASSÉ Guy & MOINET Nicolas, *Petit bréviaire contre l'intelligence superficielle*, VA, 2021.

MASSÉ Guy & THIBAULT Françoise, *Intelligence économique : un guide pour une économie de l'intelligence*, Bruxelles, De Boeck, 2001.

MOINET Nicolas, *Les sentiers de la guerre économique*. T2 – *"Soft Powers"*, VA, 2020.

MOINET Nicolas, « Le renseignement au prisme du couple agilité-paralysie », *Prospective et stratégie*, 2019/1 (n°10), pp. 13-27.

MOINET Nicolas, *Les sentiers de la guerre économique*. T1 – *L'école des nouveaux "espions"*, VA, 2018.

MOINET Nicolas, « La communication, dimension oubliée de l'intelligence économique », *Communication & Organisation*, PUB, 2012/2 (n°42).

MOINET Nicolas, *Petite histoire de l'intelligence économique. Une innovation "à la française"*, L'Harmattan, 2010.

MOINET Nicolas, « De l'information utile à la connaissance stratégique : la dimension communicationnelle de l'intelligence économique », *Communication & Organisation*, n°35, décembre 2009, pp. 214-225.

MOINET Nicolas, « L'agilité stratégique : une question de dispositif intelligent », *Vie & sciences de l'entreprise*, 2007/1-2 (n°174-175), pp. 142-155.

MOINET Nicolas, *Dispositifs intelligents et stratégies d'innovation : la dimension stratégique de l'information et de la communication dans les réseaux de la recherche-développement*, thèse de doctorat en sciences de l'information et de la communication, université de Poitiers, 1999.

NODINOT Laurent & ELHIAS Marc (alias Christian Harbulot), *Il nous faut des espions ! Le Renseignement occidental en crise*, Robert Laffont, 1988.

PAQUIN Stéphane, *Économie politique internationale*, Paris, Montchrestien, 2009.

PATINO Bruno, *La civilisation du poisson rouge : Petit traité sur le marché de l'attention*, Grasset, 2019.

PROCTOR Robert N., *Agnotology: The Making and Unmaking of Ignorance*, 1st, 2008.

RUSS Jacqueline, *Les théories du pouvoir*, Le livre de poche, 1994, 349 p.

QIAO Liang & WANG Xiangsui, *La guerre hors limites*, Payot & Rivages Éd., 2006.

SCHWARTAU Winn, *Terminal Compromise: The First Cyberterrorism Attack on the U.S.*, Interpact Pr, 2020.

SOUTOU Georges Henri, *Le sang et l'or. Les buts de guerre économiques des grandes puissances*, Fayard, 1990.

SOUTOU Georges Henri, *La guerre froide*, Fayard, 2011.

SHENK David, *Data Smog: Surviving the Information Glut*, HarperOne, 1997.

STRANGE Susan, *Le retrait de l'État : la dispersion du pouvoir dans l'économie mondiale*, Temps présent, 2011.

TALEB Nassim N., *Le cygne noir : La puissance de l'imprévisible*, Les Belles Lettres, 2008.

TRAIMOND Bernard, *L'économie n'existe pas*, Le Bord de l'Eau, 2011.

WARUSFEL Bertrand, « Les notions de défense et de sécurité en droit français », *Droit & Défense*, n°94/4, octobre 1994.

WILENSKY Harold, *Organizational Intelligence Knowledge and Policy in Government and Industry*, Basic Books, 1967.

ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, Zulma, 2022.

## Sitographie

*Sources secondaires*

https://www.frstrategie.org/programmes/observatoire-armee-de-terre-2035/concept-russe-guerre-nouvelle-generation-general-gerasimov-quelle-exploitation-pour-armee-terre-2020

https://www.portail-ie.fr/univers/defense-industrie-de-larmement-et-renseignement/2022/guerre-hybride-et-sharp-power-du-kosovo-a-lukraine-construction-dune-nouvelle-strategie-politico-militaire-russe-a-lere-gerasimov-partie-1-2/

https://www.portail-ie.fr/univers/defense-industrie-de-larmement-et-renseignement/2022/guerre-hybride-et-sharp-power-du-kosovo-a-lukraine-construction-dune-nouvelle-strategie-politico-militaire-russe-a-lere-gerasimov-partie-1-2/

https://forbiddenstories.org/fr/story-killers/team-jorge-desinformation/

https://geopoweb.fr/?LES-NOUVELLES-GUERRES-SYSTEMIQUES-NON-MILITAIRES-Par-Raphael-CHAUVANCY

https://www.lemonde.fr/archives/article/1999/06/09/les-doux-penseurs-de-la-cyberguerre_3554633_1819218.html

https://atlantico.fr/article/decryptage/it-s-the-strategy-stupid--le-nouvel-ordre-strategique-au-prisme-de-la-crise-ukrainienne-guerre-en-ukraine-russie-etats-unis-chine-otan-raphael-chauvancy

lemonde.fr/pixels/article/2019/02/18/les-deputes-britanniques-etrillent-facebook-pour-son-role-dans-les-campagnes-de-desinformation_5424886_4408996.html

wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica/

*Sources primaires*

https://www.senat.fr/rap/r20-678/r20-678_mono.html

https://www.entreprises.gouv.fr/fr/securite-economique/service-de-l-information-strategique-et-de-la-securite-economiques-sisse

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006136044/

https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/d2ie_reference_et_notion-cle-juillet.pdf

ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter

## *HACKING, COMMUNAUTÉS DE HACKERS*

BEIRNAERT-HUVELLE Jacques, DUBOURGNOUX Rémi, CLARHAUT Joffrey, EBEL Franck, *Sécurité informatique – Ethical Hacking : Apprendre l'attaque pour mieux se défendre* (6e éd.), Éd. ENI, 2022.

BERGÈRE Sylvain, *Une contre-histoire de l'internet*, film documentaire, *Premières lignes Télévision/OWNI*, 2013, 86mn.

BLANC Sabine & NOOR Ophélia, *Hackers : Bâtisseurs depuis 1959*, OWNI, 2012.

COLEMAN Gabriella, *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, 2013.

CURTET Florent (avec Sophie Garcin), *Hacke-moi si tu peux. Mémoires d'un cyperpirate repenti*, Le cherche midi, 2023.

ELAZARI Keren, *Conférence TED*, 10 juin 2014.

GUITON Amaëlle, *Hackers, au cœur de la résistance numérique*, Diable Vauvert, 2013.

HIMANEN Pekka, *L'éthique hacker et l'esprit de l'ère de l'information*, Exils, 2001.

KNAPPENBERGER Brian, *The Internet's Own Boy: The Story of Aaron Swartz*, film documentaire, 2014, 1h45.

LALLEMENT Michel, *L'Âge du faire. Hacking, travail, anarchie*, Point, 2018.

LEVY Steven, *Hackers: Heroes of the Computer Revolution*, Doubleday, 1984 ; *L'Éthique des hackers*, Globe, 2013 (trad.).

MITNICK Kevin D. & SIMON William L., *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2003.

PENALBA Pierre, *Darknet, le voyage qui fait peur. Du fantasme à la réalité*, Albin Michel, 2022.

PINARD Maxime, « L'hacktivisme dans le cyberespace : quelles réalités ? », *Revue internationale et stratégique*, 2012/3 (n°87), pp. 93-101.

SAMUEL Alexandra W., *Hacktivism and the future of political participation*, Université de Harvard, 2004.

SPAFFORD, Eugene H., « James P. Anderson: An Information Security Pioneer », *IEEE Security & Privacy Magazine*, 2008, 6(1), p. 9–9.

STOLL Clifford, *Le Nid du coucou. La longue traque d'un espion dans le labyrinthe de l'espionnage informatique*, Albin Michel, 1989.

VERLEY Samuel & PERROTIN Élodie, *Qui sont les hackers ?*, Éd. du Ricochet (livre jeunesse), 2018.

## Sitographie

https://web.archive.org/web/20220130171918/https://raidforums.com/Announcement-Database-Index-CLICK-ME

https://hackforums.net/

https://hackademics.fr/

http://phrack.org/issues/7/3.html#article

https://cultdeadcow.com/

https://www.activism.net/cypherpunk/crypto-anarchy.html

https://www.activism.net/cypherpunk/manifesto.html

https://www.harvardmagazine.com/2000/01/code-is-law-html

http://tmrc.mit.edu/hackers-ref.html

http://catb.org/~esr/jargon/html/H/hacker.html

https://archive.wikiwix.com/cache/index2.php?url=http://www.volle.com/lectures/citations/hackersethic.htm

https://www.digibarn.com/collections/newsletters/homebrew/V2_01/homebrew_V2_01_p2.jpg

https://scinfolex.com/2014/01/24/comment-code-is-law-sest-renverse-en-law-is-code/

https://opensource.org/

https://www.root-me.org/

https://web.archive.org/web/20220521090918/https://ctf.404ctf.fr/

https://www.dghack.fr/

https://www.login-securite.com/2019/02/22/le-pentest-de-a-a-z-methodologie-et-bonnes-pratiques-pour-securiser-son-si/

https://portswigger.net/burp

https://fr.tenable.com/products/nessus

https://www.parrotsec.org/

https://www.kali.org/

https://www.lemonde.fr/archives/article/2002/09/30/garde-a-vue-pour-les-dirigeants-de-hackerz-voice_292460_1819218.html

https://hzv.fr/

### *OSINT*

ALLOING Camille, « La sousveillance. Vers un renseignement ordinaire », *in* « Le renseignement, un monde fermé dans une société ouverte », *Hermès*, 2016/3 (n°76), pp. 68-73.

BAZZELL Michael, *OSINT Techniques: Resources for Uncovering Online Information*, Tenth, 2023.

DEBLIQUY Pierre-Yves, *Chercher n'est pas trouver*, Édipro, 2014.

DYLEWSKI Philippe, *Le Renseignement Offensif : 300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs*, Agakure, 2021.

FRANCIS Fanch, *De la prédiction à la détection d'évènements : L'analyse des mégadonnées au service du renseignement de sources ouvertes*, thèse de doctorat en sciences de l'information et de la communication, université de Lille, 2019.

LIMONIER Kevin, & AUDINET Maxime (dir.), « OSINT, enquêtes et terrains numériques », *Hérodote* (n°186), La découverte, 2022.

LONG Johnny, *Google Hacking. Mettez vos données sensibles à l'abri des moteurs de recherches,* Dunod, 2005.

MARTIN (LTC), *OSINT : L'Art de collecter l'information ouverte*, Éd. du Château, 2023.

## Sitographie

https://ozint.eu/

https://openfacto.fr/

https://osintfr.com/fr

https://www.cxo-community.com/2018/06/ciberinteligencia-del-osint-al-cybint.html#.WylktqgUtlo.linkedin

https://www.robertmlee.org/cyber-intelligence-part-1-an-introduction-to-cyber-intelligence/

### *RENSEIGNEMENT*

BAUD Jacques, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002.

BEAU Francis, *Le renseignement au prisme des sciences de l'information*, thèse de doctorat en sciences de l'information et de la communication, université de Valenciennes, 2019.

BULINGE Franck et MOINET Nicolas (dir.), « Le renseignement, un monde fermé dans une société ouverte », *Hermès*, 2016/3 (n°76).

BULINGE Franck, *De l'espionnage au renseignement. La France à l'âge de l'information*, Vuibert, 2012.

CARLESON J.C., *Work Like a Spy: Business Tips from a Former CIA Officer*, Portfolio, 2013.

CHOPIN Olivier & OUDET Benjamin, *Renseignement et sécurité*, Armand Colin, 2019.

GIOE David, STEVENS Tim, GOODMAN Michael S., « Intelligence in Cyber Era: Evolution or Revolution? » *Political Science Quarterly*, 2020, pp. 191-224.

GUYAUX Jean (général), *L'espion des sciences*, Flammarion, 2002.

JAVERS Eamon, *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage*, Harper Business, 2010.

JORDANOV Alex, *Les guerres de l'ombre de la DGSI - Plongée au cœur des services secrets français*, Nouveaux mondes Éditions, 2019.

LACOSTE Pierre, « Quel renseignement pour le XXIe siècle ? », *Actes du colloque au Carré des Sciences du 3 avril 2001*, Panazol, Éditions Lavauzelle, 2021.

LACOSTE Pierre & THUAL François, *Services secrets et géopolitique*, Lavauzelle, 2001.

PECH Yannick, « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », *Prospective et stratégie*, 2019/1 (n°10), pp. 73-102.

PECH Yannick, *L'influence du renseignement dans la formulation de la politique étrangère depuis 1991. Approche comparée de l'impact des cultures du renseignement américaine et française sur le processus décisionnel*, mémoire de M2 en science politique-Relations internationales, université de Lyon 3, 2013.

STEELE Robert D., *On Intelligence: Spies and Secrecy in an Open World*, OSS International Press, 2016.

ZIMMER Terry, *Le renseignement humain à l'ère numérique*, VA, 2018.

## *ÉPISTÉMOLOGIE, MÉTHODOLOGIE, SCIENCES DE L'INFORMATION ET DE LA COMMUNICATION*

DACHEUX Éric (dir.), *Les sciences de l'information et de la communication*, CNRS Éditions, 2009.

FOUCAULT Michel, *Surveiller et punir. La naissance de la prison*, Gallimard, 1975.

HALLÉE, Yves & GARNEAU, Julie M. É., « L'abduction comme mode d'inférence et méthode de recherche : de l'origine à aujourd'hui », *Recherches qualitatives*, 38(1), 2019, pp. 124–140.

HEATON Janet, *Reworking Qualitative Data*, Sage Publications, 2004.

KUHN Thomas S., *La Structure des révolutions scientifiques*, Flammarion, 1992 (rééd. 2008).

LEGAVRE Jean-Baptiste et RIEFFEL Rémy, *Les 100 mots des sciences de l'information et de la communication*, « Que sais-je ? », PUF, 2017.

MATTELART Armand, *Histoire de la société de l'information*, La Découverte, (5e éd.), 2018.

MATTELART Armand, *La mondialisation de la communication*, PUF – Que sais-je ?, 1996, pp. 3-4.

MORIN Edgard, *Les Sept savoirs nécessaires à l'éducation du futur*, Points, 2015.

MORIN Edgard, *Introduction à la pensée complexe*, Points, 2014.

MORIN Edgard, *La Méthode*, T.1 & T.2, Seuil, 2008.

MOSCAROLA Jean, *Faire parler les données. Méthodologie quantitatives et qualitatives*, EMS Éditions, 2018.

MUCCHIELLI Alex, « Pour des recherches en communication », in "La recherche en communication", *Communication & organisation*, ISIC-GRECO/O, n°10, 1996.

NUÑEZ MOSCOSO Javier, « Et si l'on osait une épistémologie de la découverte ? La démarche abductive au service de l'analyse du travail enseignant », *Penser l'éducation*, 33, 2013, pp. 57-80.

PERAYA Daniel, *in* « Le dispositif. Entre usage et concept », *Hermès*, 1999/3 (n°25), pp. 153-167.

VARELA Fernando, « Constructivisme et énaction », *École thématique CNRS*, ARCo, 2006.

WOLTON Dominique, « Communication, incommunication et acommunication », in *Les incommunications*, *Hermès*, 2019/2 (n°84), pp. 200-205.

## Sitographie

https://mica.u-bordeaux-montaigne.fr/dussarps-clement/

## *ŒUVRES DE FICTION*

DICK Philip K., *Do Androids Dream of Electric Sheep?*, Doubleday, 1968 (roman).

GIBSON William, *Neuromancien*, La Découverte, 1985 (roman).

ŌTOMO Katsuhiro, *Akira*, film d'animation, Tokyo Movie Shinsha, Japon, 1988, 124mn.

OSHII Mamoru, *Ghost in the Shell*, film d'animation, Production I.G, Bandai Visual, Manga Entertainment, Japon/Royaume-Uni, 1995, 82mn.

SANDERS Rupert, *Ghost in the Shell*, film d'animation, Paramount Pictures, Amblin Partners, DreamWorks Pictures, Arad Productions, Reliance Entertainment, Steven Paul Productions, États-Unis/Hong-Kong/Inde/Chine, 2017, 107mn.

SCOTT Ridley, *Blade Runner*, film cinématographique, Warner Bros, The Ladd Company, Shaw Brothers, États-Unis/Hong-Kong, 1982, 111-117mn.

SOFTLEY Iain, *Hackers*, film cinématographique, United Artists, États-Unis, 1995, 107mn.

# TABLE DES ILLUSTRATIONS

# TABLE DES MATIÈRES