Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie

Evelyne K Akoto

Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie

EVELYNE AKOTO*

La *Charte des Nations Unies*, rédigée pour faire face aux dangers qu'impliquent les conflits de forte intensité, ne semble pas, de prime abord, pouvoir répondre aux défis juridiques que présentent l'avènement et le développement fulgurant des nouvelles technologies. Les infrastructures informatiques étant devenues les points névralgiques de nos sociétés modernes, les États sont désormais vulnérables à une nouvelle menace protéiforme et sournoise : la cyberattaque étatique. En effet, si la subversion et les conflits de basse intensité étaient les méthodes privilégiées des grandes puissances pendant la Guerre froide, l'acquisition progressive de l'arme nucléaire par de plus en plus de pays a fait des cyberattaques étatiques l'outil parfait pour atteindre les mêmes objectifs d'hégémonie.

Cet article va ainsi examiner si une cyberattaque étatique peut être qualifiée d'acte d'agression sur la base des critères d'analyse fournis dans la *Résolution 3314* de l'Assemblée générale des Nations Unies. La première partie, publiée dans le présent numéro, sera consacrée à une courte présentation de la notion de « cyberattaque étatique » et une illustration du concept par les descriptions des cyberattaques qu'ont connues l'Estonie en 2007, la Géorgie en 2008 et l'Iran en 2011. Nous conclurons cette partie par un exposé succinct des défis posés par les cyberattaques étatiques en matière de maintien de la paix et de la sécurité internationales. La seconde partie, qui paraîtra dans le deuxième numéro du présent volume, analysera les cyberattaques étatiques à la lueur des normes internationales relatives à la prohibition de l'agression.

The *Charter of the United Nations*, drafted to address the perils of high intensity conflicts, does not seem, at first glance, capable of answering the legal challenges raised by the rapid conception and development of new technologies. Information technology infrastructures, having become the hotspots of our modern societies, have now rendered states vulnerable to a new protean and insidious threat: the state cyberattack. Indeed, if subversion and low intensity conflicts were the chosen means of the great powers during the Cold War, the buildup of nuclear capabilities by more and more states, has made state cyberattacks, the perfect tool to reach the same hegemonic ambitions.

This article will examine whether a state cyberattack qualifies as an act of aggression according to the criteria set out by United Nations General Assembly *Resolution 3314*. The first section, published in the present issue, will provide an overview of the notion of "state cyberattack" and will illustrate it with the description of the cyberattacks against Estonia in 2007, Georgia in 2008 and Iran in 2011. In conclusion, a brief presentation of the challenges raised by state cyberattacks with regards to the maintenance of international peace and security. The second section, to be published in the second issue of the present volume, will review state-sponsored cyberattacks in light of the international norms pertaining to the prohibition of aggression.

* Dotée d'une formation en droit et en économie financière, Evelyne Akoto est chargée de cours en droit international public à la Section de droit civil de l'Université d'Ottawa. Elle s'intéresse à divers domaines d'application juridique, allant de la promotion de l'état de droit dans les États fragiles, notamment en situation post-conflit, à la protection des droits de l'homme, en passant par les règles encadrant l'usage de la force dans les relations internationales. L'auteure aimerait vivement remercier Me Fannie Lafontaine, professeure agrégée de droit à l'université Laval et titulaire de la Chaire de recherche du Canada sur la justice internationale pénale et les droits fondamentaux, pour ses conseils avisés lors de la rédaction de l'essai de maîtrise ayant mené à la publication de cet article.

Table des matières

Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie

EVELYNE AKOTO

I. INTRODUCTION

« Si les réseaux vitaux d'information cessaient de fonctionner, une société de l'information serait paralysée et sombrerait vite dans le chaos » [notre traduction][1].

La *Charte des Nations Unies* (ci-après « *Charte* »)[2], rédigée pour faire face aux dangers qu'impliquent des conflits traditionnels et de forte intensité comme les Première et Seconde Guerres mondiales ne semble pas, de prime abord, pouvoir répondre aux défis juridiques que représentent l'avènement et le développement fulgurant des nouvelles technologies. En effet, les infrastructures informatiques sont devenues les points névralgiques de nos sociétés modernes. Les entreprises privées, les administrations publiques, la gestion des trafics aériens, routiers et ferroviaires, les centrales électriques et de distribution d'eau et les nouvelles armes de guerre telles que les drones fonctionnent toutes à l'aide d'ordinateurs connectés à des réseaux au maillage si diffus qu'ils exposent les États à une nouvelle menace polymorphe et particulièrement furtive : la cyberattaque étatique.

Les cyberattaques étatiques pourraient être sommairement décrites comme des offensives attribuables à un État et menées contre les réseaux informatiques d'un autre pays afin d'occasionner des perturbations dans le fonctionnement des activités et services publics ou privés de l'État cible ; ce qui provoque des désagréments pour le quotidien des ressortissants dudit pays. Elles présentent « deux types de préoccupations » [emphases omises][3] : d'une part, les risques liés à l'attaque des « services essentiels au fonctionnement [d'un] pays ou à sa défense »

---

1 Todd A Morth, « Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter » (1998) 30 Case W Res J Intl L 567 à la p 568 [Morth].

2 *Charte des Nations Unies*, 26 juin 1945, RT Can 1945 n° 7 préambule [*Charte*].

3 France, Sénat, *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, par Jean-Marie Bockel, rapport n° 681 (18 juillet 2012) à la p 11 [France, *Rapport d'information du Sénat*].

[emphases omises][4] et d'autre part, les enjeux et défis posés par « la protection des informations sensibles du point de vue politique, militaire ou économique, face à des techniques d'intrusion informatique de plus en plus sophistiquées » [emphases omises][5]. En effet, en raison de leur caractère très subreptice, les cyberattaques remettent en question les notions traditionnelles de frontières[6], ces dernières étant coutumièrement inviolables. Dorénavant, la force cinétique n'est plus nécessaire pour engendrer des dommages importants, ceux-ci pouvant d'ailleurs ne pas être de nature physique, si telle est l'intention de l'auteur de l'attaque informatique.

La grande majorité des activités informatiques de nature malveillante ont lieu en temps de paix[7], ce qui peut souvent prêter à confusion quant à ce qu'englobent les cyberattaques étatiques. C'est pourquoi, avant de décrire l'objet de cet article, nous allons procéder à quelques distinctions définitionnelles, eu égard à la multitude d'activités illégales pouvant prendre place dans le cyberespace. L'article ne traitera pas de la cybercriminalité qui comprend plusieurs actions interdites telles que la pornographie infantile, l'hameçonnage, l'envoi de pourriels, etc., et régies par le droit pénal national[8]. Il n'abordera pas non plus le cyberespionnage industriel qui est la copie de secrets industriels afin d'obtenir un avantage compétitif[9]. L'exposé ne portera pas sur le cyberterrorisme qui constitue la conduite dans le cyberespace d'activités terroristes par des groupes armés transnationaux, agissant en leur nom et pour leur propre compte[10].

Si la subversion et les conflits de basse intensité étaient les méthodes privilégiées des grandes puissances pendant la Guerre froide, l'acquisition progressive de l'arme nucléaire par de plus en plus de pays, a fait des cyberattaques étatiques l'outil parfait pour atteindre les mêmes objectifs d'hégémonie[11]. Les

---

4 *Ibid.*

5 *Ibid*.

6 Jonathan A Ophardt, « Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield » (2010) 3 Duke L & Tech Rev aux para 1, 29 [Ophardt].

7 Katharina Ziolkowski, dir, *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn (Estonie), NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013 à la p XV [Ziolkowski, *Peacetime Regime*].

8 Voir par ex Éric Freyssinet, *La cybercriminalité en mouvement*, Cachan, Hermès-Lavoisier, 2012 ; Francis Fortin, dir, *Cybercriminalité : Entre inconduite et crime organisé*, Canada, Presses internationales Polytechnique et Sûreté du Québec, 2013.

9 Voir par ex Daniel J Benny, *Industrial Espionage: Developing a Counterespionage Program*, Boca Raton (Fla), CRC Press Taylor & Francis Group, 2014 ; Will Gragido, John Pirc et Russ Rogers, *Cybercrime and Espionage: An Analysis of Subversive Multivector Threats*, Burlington (Mass), Elsevier, 2011. Voir notamment Ira Winkler, *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day*, Indianapolis, Wiley Publishing, 2005.

10 Voir par ex Imran Awan et Brian Blakemore, dir, *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, Farnham, Ashgate, 2012.

11 Matthew C Waxman, « Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) » (2011) 36:1 Yale J Intl L 421 à la p 441 [Waxman, « Cyber-Attacks »]. Comparer Choe Sang-Hun, « Computer Networks in South Korea Are Paralyzed in Cyberattacks », *The New York Times* (20 mars 2013), en ligne : <www.nytimes.com/2013/03/21/world/asia/south-korea-computer-

États-Unis ont déclaré qu'ils pourraient entreprendre des actions militaires au titre de la légitime défense[12] ou des représailles[13] en réponse à des cyberattaques prétendument commanditées par d'autres pays. Une telle prise de position pose la question de la qualification d'une cyberattaque étatique en droit international public : s'agit-il d'un recours à la force ? D'un acte d'agression contre un autre État ? À l'instar de la Guerre froide avec ses guerres provoquées (par agents interposés), assiste-t-on de nouveau à des violations insidieuses des principes des Nations Unies ne pouvant faire l'objet d'aucune condamnation internationale, en l'absence de toute *casus belli* ? C'est à ces questions que va tenter de répondre cet article dont le premier volet exposé dans ce numéro, sera consacré à une présentation de la notion de « cyberattaque étatique », d'une illustration du concept par les descriptions des cyberattaques qu'ont connues l'Estonie en 2007, la Géorgie en 2008 et l'Iran en 2011, ces trois incidents cybernétiques ayant été le plus médiatisés jusqu'à maintenant sur le plan international, à notre connaissance. Nous conclurons cette partie par une description sommaire des défis posés par les cyberattaques étatiques en matière de maintien de la paix et de la sécurité internationales.

---

network-crashes.html?ref=davidesanger> ; The Associated Press, « Chinese internet address involved in S. Korea cyberattack: South Korean regulators still investigating attack on banks, media outlets », *CBC* (21 mars 2013), en ligne : <www.cbc.ca/news/world/chinese-internet-address-involved-in-s-korean-cyberattack-1.1346290> [AP, « Chinese internet »] ; Justin McCurry, « North Korea readies missile launch as fears of a covert cyberwar grow », *The Guardian* (6 avril 2013), en ligne : <www.theguardian.com/world/2013/apr/07/north-korea-missile-launch-cyberwar-fears?view=mobile> [McCurry] (au sujet des cyberattaques qu'a subies la Corée du Sud au printemps 2013 sous fond de tensions diplomatiques entre Washington et Pyongyang au sujet des essais nucléaires nord-coréens). Voir aussi Barton Gellman et Ellen Nakashima, « U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show », *The Washington Post* (30 août 2013), en ligne : <www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html> [Gellman et Nakashima, « U.S. spy »] ; Duncan Gardham, « Hackers recruited to fight 'new cold war' », *The Telegraph* (26 juin 2009), en ligne : <www.telegraph.co.uk/technology/news/5637243/Hackers-recruited-to-fight-new-cold-war.html> [Gardham] ; Duncan Gardham, « Cold war enemies Russia and China launch a cyber attack every day », *The Telegraph* (4 décembre 2009), en ligne : <www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html>.

12 Harold Hongju Koh, « International Law in Cyberspace » USCYBERCOM Inter-Agency Legal Conference, présentée à Fort Meade (Md), 18 septembre 2012 [non publiée], en ligne : <www.state.gov/s/l/releases/remarks/197924.htm>. Voir par ex Ellen Nakashima, « Cyberattacks could trigger self-defense rule, U.S. official says », *The Washington Post* (18 septembre 2012), en ligne : <www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html?wpisrc=emailtoafriend> [Nakashima, « Cyberattacks »] ; « US looking at action against China cyber attacks », *The Sydney Morning Herald* (1 février 2013), en ligne : <www.smh.com.au/it-pro/security-it/us-looking-at-action-against-china-cyber-attacks-20130201-2dpgm.html> [« US looking », *The Sydney Morning Herald*].

13 David E Sanger, « In Cyberspace, New Cold War », *The New York Times* (24 février 2013), en ligne : <www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?ref=davidesanger&_r=0> [Sanger, « In Cyberspace »].

II. QUELQUES NOTIONS DE BASE SUR LA CYBERATTAQUE ÉTATIQUE

Le mot « cyberattaque » est un néologisme formé à partir du préfixe « cyber »[14] et du substantif « attaque ». Le cyberespace représente un espace universel « constitué d'un réseau interdépendant d'infrastructures informatiques comprenant l'Internet[15], les réseaux de télécommunications, les systèmes informatiques ainsi que les processeurs et les contrôleurs intégrés » [notre traduction][16]. Entièrement créé par l'homme[17], il n'est pas restreint par des frontières et ressemble sur ce dernier point à la haute mer et à l'espace extra-atmosphérique[18]. Il ne relève donc pas dans son entièreté de la compétence d'un seul État ou d'un groupe d'États[19], ce

---

14 Québec, Office québécois de la langue française, *Bibliothèque virtuelle*, Québec, Gouvernement du Québec, 2002, *sub verbo* « cyber », en ligne : <www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/2075010.html> [OQLF] (« [p]réfixe que l'on ajoute à un mot existant pour en transposer la réalité dans le cyberespace ou pour l'associer à celui-ci »).

15 Dans le cadre de cet article, lorsque nous évoquerons le réseau Internet dans sa globalité, nous utiliserons une majuscule pour écrire le substantif « Internet », la minuscule sera employée quand nous apposerons le substantif comme adjectif épithète à un nom.

16 É-U, Department of Commerce, *Glossary of Key Information Security Terms*, Richard Kissel, dir, United States, National Institute of Standards and Technology Interagency Report 7298 Revision 1, 2011 à la p 57 [Kissel, *Glossary*]. Voir aussi Canada, Ministère des Travaux publics et des Services gouvernementaux, *La banque de données terminologiques et linguistiques du gouvernement du Canada*, Terminus Plus, 2014 *sub verbo* « cyberspace », en ligne : <www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&index=alt&__index=alt&srchtxt=CYBERESPACE&comencsrch.x=7&comencsrch.y=4> [Termium Plus] (« [m]onde numérique construit par des ordinateurs et des réseaux d'ordinateurs, dans lequel coexistent des gens et des ordinateurs, et qui englobe toutes les zones d'activité en ligne […] Depuis 1993, "cyberespace" a subi une extension de sens : restreint au début à la réalité virtuelle, il englobe aujourd'hui les communications sur Internet, comme en anglais »). Comparer Nils Melzer, « Cyberwarfare and International Law », en ligne : (2011) United Nations Institute for Disarmament Research Resources à la p 4 <www.unidir.org/publications/emerging-security-threats> [Melzer, « Cyberwarfare »] ; Wolff Heintschel von Heinegg, « Legal Implications of Territorial Sovereignty in Cyberspace » dans C Czosseck, R Ottis et K Ziolkowski, dir, *2012 4th International Conference on Cyber Conflict*, Tallinn (Estonie), NATO Cooperative Cyber Defence Center of Excellence Publications, 2012 [Czosseck, Ottis et Ziolkowski, *2012*], 7 à la p 9 [von Heinegg]. Voir aussi Canada, Ministère de la Sécurité publique, *Stratégie de cybersécurité du Canada : renforcer le Canada et accroître sa prospérité*, Gouvernement du Canada 2010 à la p 2 [Canada, *Stratégie de cybersécurité*]. Tout au long de cet article, le préfixe « cyber » sera utilisé avec plusieurs mots qui ne seront pas forcément définis. Il faudra juste comprendre que ces mots conservent leur acception d'origine, à la seule différence que leur emploi est considéré par rapport à l'environnement que représente le cyberespace.

17 Chris C Demchak et Peter Dombrowski, « Rise of a Cybered Westphalian Age » (2011) 5:1 Strategic Studies Quarterly 32 à la p 35. Voir généralement Fred Schreier, « On Cyberwarfare » (2012) 7 Democratic Control of Armed Forces Horizon 2015 Working Paper, (DCAF.ch), en ligne : <www.dcaf.ch/Publications/On-Cyberwarfare> aux pp 93–106 [Schreier].

18 Voir généralement Benedikt Pirker, « Territorial Sovereignty and Integrity and the Challenges of Cyberspace » dans Ziolkowski, *Peacetime Regime*, *supra* note 7, 189 aux pp 194–195 [Pirker].

19 Voir généralement Schreier, *supra* note 17 aux pp 93–106 ; Michael N Schmitt, dir, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge (NY), Cambridge University Press, 2013 aux pp 18–21 [Schmitt, *Tallinn Manual*] (voir la règle 2) ; Katharina Ziolkowski, « General Principles of International Law as Applicable in Cyberspace » dans Ziolkowski, *Peacetime Regime*, *supra* note 7, 135 à la p 162 [Ziolkowski, « General Principles of IL »]. Voir aussi Jeffrey Carr, *Inside Cyber Warfare*, 2e éd, Sebastopol (Cal), O'Reilly, 2011 à la p 177 [Carr, *Inside Cyber*].

qui en fait un bien commun planétaire[20]. En ce qui concerne la racine « attaque », elle a des emplois différents selon que l'on se place sur le plan juridicomilitaire[21] ou informatique. En informatique, une attaque représente toute tentative d'accès non autorisé à un système de services, à des ressources ou à une information ; ou toute tentative visant à compromettre l'intégrité du système[22]. Ainsi selon cette définition que nous allons retenir dans le cadre de cet article, une attaque cinétique telle que l'accès à l'aide d'explosifs de la salle de serveurs d'une entreprise constituerait un exemple d'attaque informatique[23].

Une cyberattaque est donc un terme générique qualifiant les attaques informatiques menées uniquement dans et par le cyberespace[24]. Ce type d'attaque cherche à exploiter les failles pouvant émerger ou résulter de l'accès d'un usager au cyberespace[25]. Le but d'une cyberattaque est de perturber, neutraliser, détruire[26]

---

20 Voir notamment Schmitt, *Tallinn Manual*, *supra* note 19 aux pp 15–18 (voir la règle 1) ; Pirker, *supra* note 18 aux pp 195–96. Comparer *Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies*, Rés AG 2625, Doc off AG NU, 25e sess, Doc NU A/8082 (1970) préambule au para 7 ; *Contra* Ronald J Deibert, *Black Code: Inside the Battle for Cyberspace*, Toronto, Signal McClelland & Steward, 2013 à la p 234.

21 Sur le plan juridique, s'il n'apparaît nulle part dans la version française de la *Charte*, le mot « attaque » figure à l'article 51 de la version anglaise de celle-ci dans l'expression « armed attack » qui a été traduite en français par « agression armée ». Dans le contexte des relations internationales, une attaque en temps de paix est un acte de violence armée intenté à l'encontre de la souveraineté d'un État et qui peut, sous certaines conditions, être qualifié d'agression et, le cas échéant, ouvrir droit à l'exercice du droit de légitime défense (voir notamment *Charte*, *supra* note 2, art 51). Voir aussi Michael N Schmitt « "Attack" as a Term of Art in International Law: The Cyber Operations Context » dans Czosseck, Ottis et Ziolkowski, *2012*, *supra* note 16, 283 à la p 285. Selon le droit des conflits armés, l'attaque est un type particulier d'opération militaire « sans rapport avec la notion d'agression ou de premier recours à la violence » (voir notamment le commentaire de l'article 49 dans Jean de Preux et al, *Commentaire des Protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949*, Genève, Comité international de la Croix-Rouge, 1987, en ligne : <www.icrc.org/applic/ihl/dih.nsf/Comment.xsp?viewComments=LookUpCOMART&articleUNID=E111A6 EAF5554AEBC12563BD002C2477>, aux para 1880, 1882 ; *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)*, 8 juin 1977, 1125 RTNU 3 art 49 (entrée en vigueur : 7 décembre 1978)).

22 Kissel, *Glossary*, *supra* note 16 à la p 12. Voir par ex OQLF, *supra* note 14, *sub verbo* « attaque informatique », en ligne : <gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2074420> (« [t]entative de violation de la sécurité des données »).

23 Voir par ex Oona A Hathaway et al, « The Law of Cyber-Attack » (2012) 100 Cal L Rev 817 à la p 826 [Hathaway et al].

24 Kissel, *Glossary*, *supra* note 16 à la p 56 ; Canada, *Stratégie de cybersécurité*, *supra* note 16 à la p 3. Voir aussi Termium Plus, *supra* note 16, *sub verbo* « cyberattack » en ligne : <www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&index=alt&__index=alt&srchtxt=cyber+attaque&comencsrch.x=0&comencsrch.y=0>. Voir toutefois Hathaway et al, *supra* note 23 à la p 826 (les auteurs proposent une définition de la cyberattaque qui inclut aussi les actions cinétiques entreprises contre des installations informatiques telles que le bombardement aérien de l'unité d'information opérationnelle et de cyber commandement d'un État) ; Schmitt, *Tallinn Manual*, *supra* note 19 aux pp 106–110 (voir la règle 30), 258 (*sub verbo* « cyber operations »).

25 Kissel, *Glossary*, *supra* note 16 à la p 56.

26 *Ibid* ; Melzer, « Cyberwarfare », *supra* note 16 à la p 5. Voir aussi Organisation du Traité de l'Atlantique Nord, *Glossaire OTAN de termes et définitions (Anglais et Français)*, éd 2014, Agence OTAN de Normalisation, 2014, *sub verbo* « attaque de réseaux informatiques », en ligne : <nsa.nato.int/nsa/zPublic/

ou contrôler de façon malveillante l'infrastructure informatique de la cible ou d'en détruire l'intégrité des données ou voler des informations protégées[27]. Par conséquent, nous estimons que la cyberattaque englobe également les activités d'exploitation non autorisée des réseaux informatiques (*computer network exploitation*)[28]. Ces activités désignent toute tentative d'accès non permis aux données d'un réseau informatique ou au réseau lui-même en vue de s'approprier et d'analyser des données sensibles[29].

Les cyberattaques peuvent être parrainées, organisées, coordonnées et réalisées par des personnes[30] physiques, morales ou des États[31] ; elles ont pour cible aussi bien des compagnies et établissements privés que publics, de même que des particuliers[32]. En juin 2012, la compagnie Google alertait les usagers de son service de messagerie électronique Gmail des risques de cyberattaques commanditées par des États auxquels étaient exposés leurs comptes[33]. Qu'entend-on donc par « cyberattaque étatique » ?

---

ap/aap6/AAP-6.pdf> [OTAN, *Glossaire*] (« Note: A computer network attack is a type of cyber attack » à la p 2-C-11) ; Termium Plus, *supra* note 16, *sub verbo* « cyberattack ».

27 Melzer, « Cyberwarfare », *supra* note 16 à la p 5 ; Marco Roscini, « World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force » (2010) 14 Max Planck YB United Nations L 85 à la p 93 [Roscini] ; Herbert S Lin, « Offensive Cyber Operations and the Use of Force » (2010) 4:1 J National Security L & Policy 63 à la p 63 ; Matthew C Waxman, « Cyber Attacks as "Force" under UN Charter Article 2(4) » (2011) 87 Intl L Studies 43 à la p 43. Voir aussi Canada, *Stratégie de cybersécurité*, *supra* note 16 à la p 3 ; France, *Prévention des R!sques Majeurs*, en ligne : <http://www.risques.gouv.fr/menaces-terroristes/focus-cyber-securite> ; Termium Plus, *supra* note 16, *sub verbo* « cyberattaques », en ligne : <www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&index=alt>. Voir par ex Gellman et Nakashima, « U.S. spy », *supra* note 11. *Contra* Schmitt, *Tallinn Manual*, *supra* note 19 aux pp 106-110 (voir la règle 30), 258 (*sub verbo* « cyber operations »).

28 Voir OTAN, *Glossaire*, *supra* note 26, *sub verbo* « exploitation de réseau informatique » à la p 2-C-11 ; Melzer, « Cyberwarfare », *supra* note 16 à la p 5 ; Roscini, *supra* note 27 à la p 92. Voir aussi R-U, Houses of Parliament, *Cybersecurity in the UK* (PostNote n° 389), Londres, Parliamentary office of science and technology, 2011 à la p 2. Voir toutefois Katharina Ziolkowski, « Peacetime Cyber Espionage – New Tendencies in Public International Law » dans Ziolkowski, *Peacetime Regime*, *supra* note 7, 425 à la page 428 [Ziolkowski, « Peacetime Cyber Espionage »].

29 Voir Kissel, *Glossary*, *supra* note 16 à la p 41 ; OTAN, *Glossaire*, *supra* note 26, *sub verbo* « exploitation de réseau informatique » à la page 3-E-11. Voir par ex Gellman et Naskashima, « U.S. spy », *supra* note 11.

30 Voir généralement Carr, *Inside Cyber*, *supra* note 19 ; Gregory J Rattray et Jason Healey, « Chapter V: Non-State actors and cyber conflict » dans Kristin M Lord et Travis Sharp, dir, *America's Cyber Future: Security and Prosperity in the Information Age Volume II*, Washington (DC), Center for a New American Security, 2011, 65, en ligne : <www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf>.

31 Voir généralement Carr, *Inside Cyber*, *supra* note 19. Voir aussi France, *Rapport d'information du Sénat*, *supra* note 3 à la p 36 ; Canada, *Stratégie de cybersécurité*, *supra* note 16 à la p 5.

32 Voir France, *Rapport d'information du Sénat*, *supra* note 3 à la p 29 ; Canada, *Stratégie de cybersécurité*, *supra* note 16. Voir par ex Gellman et Naskashima, « U.S. spy », *supra* note 11.

33 Nicole Perlroth, « Google Issues New Warning for State-Sponsored Attacks », *The New York Times* (5 juin 2012), en ligne : <bits.blogs.nytimes.com/2012/06/05/google-issues-new-warning-for-state-sponsored-attacks/> ; Hayley Tsukayama et Ellen Nakashima, « Google to alert users about state-sponsored attacks », *The Washington Post* (5 juin 2012), en ligne : <www.washingtonpost.com/business/economy/google-to-alert-users-about-state-sponsored-attacks/2012/06/05/gJQAzS-R8GV_story.html>. Voir aussi Nicole Perlroth, « Google Warns of New State-Sponsored Cyberattack Targets », *The New York Times* (2 octobre 2012), en ligne : <bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets/?_&_r=0>.

A. Définition et caractéristiques d'une cyberattaque étatique

Le cyberespace est désormais considéré comme un nouveau champ de bataille[34], à l'instar de la terre, la mer, l'air et l'espace extra-atmosphérique. Les cyberattaques étatiques sont souvent qualifiées à tort dans la presse, d'actes de cyberguerre[35]. La cyberguerre est la conduite, dans un contexte de conflit armé[36], d'activités militaires à l'aide de moyens et de méthodes numériques dans le cyberespace ; elle comprend aussi bien des activités offensives que défensives des infrastructures informatiques[37]. Par conséquent, en l'absence de tout conflit armé opposant deux États, toute cyberattaque opposant lesdits États est considérée avoir eu lieu en temps de paix[38] et n'est donc pas un acte de cyberguerre.

---

34 Voir Scott J Shackelford et Richard B Andres, « State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem » (2010) 42:1 Geo J Intl L 971 à la p 974 ; Paul Cornish et al, « On Cyber Warfare », en ligne : (2010) Chatham House à la p 11 <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf> [Cornish et al] ; Kenneth Geers et al, « World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks », en ligne : (2013) FireEye à la p 5 <https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-wwc-report.pdf> [Geers et al]. Voir par ex « Cyberwar: War in the fifth domain », *The Economist* (1 juillet 2010), en ligne : <www.economist.com/node/16478792>. *Contra* Carr, *Inside Cyber*, *supra* note 19 à la p xiii ; Martin C Libicki, « Cyberspace Is Not a Warfighting Domain » (2012) 8:2 I/S: A Journal of Law and Policy for the Information Society 321.

35 « Estonia hit by 'Moscow cyber war' », *BBC News* (17 mai 2007), en ligne : <news.bbc.co.uk/go/pr/fr/-/2/hi/europe/6665145.stm> [« Estonia hit », *BBC News*] ; Ian Traynor, « Russia accused of unleashing cyberwar to disable Estonia », *The Guardian* (17 mai 2007), en ligne : <www.theguardian.com/world/2007/may/17/topstories3.russia?mobile-redirect=false> [Traynor, « Russia accused »].

36 Il est important de distinguer la notion d'« agression armée » de celle de « conflit armé », les deux concepts étant souvent substitués l'un à l'autre, de façon erronée. Pour qu'un conflit armé soit qualifié d'agression armée, il faut que des actes de violence aient eu lieu entre deux États, qu'une frontière internationale ait été violée lors de la commission desdits actes et que ceux-ci soient graves de par leurs dimensions et effets. Tout emploi de la force ne veut pas nécessairement dire qu'un conflit armé a lieu et ce ne sont pas tous les actes de guerre qui sous-entendent un emploi de la force. Par exemple, la capture d'un soldat étranger lors d'un incident frontalier donne lieu à l'application du *jus in bello* donc à la reconnaissance d'un éventuel conflit armé international, mais on n'est pas en présence d'une agression armée (voir notamment Keiichiro Okimoto, *The Distinction and Relationship between Jus ad Bellum and Jus in Bello*, Oxford, Hart Publishing, 2011 aux pp 45, 48–50). Par conséquent, l'existence d'un conflit armé international ne dépend pas nécessairement d'un emploi de la force entre États, mais plutôt de l'existence d'actes de violence au sens du *jus in bello* (voir les *Conventions de Genève*, 12 août 1949, 75 RTNU 31, 85, 135, 287, art 2). Voir aussi Walter Gary Sharp, *CyberSpace and the Use of Force*, Falls Church (Va), Aegis Research Corporation, 1999 à la p 59 [Sharp] (la guerre représente une situation conflictuelle *de jure* tandis que le conflit armé désigne une situation *de facto*).

37 Voir notamment Schmitt, *Tallinn Manual*, *supra* note 19 à la p 75 (voir la règle 20).

38 Voir aussi Ziolkowski, *Peacetime Regime*, *supra* note 7 à la p XV. Du point de vue du *jus in bello*, il serait intéressant de savoir si une cyberattaque étatique, exécutée indépendamment de tout conflit armé international conventionnel, peut être considérée comme un conflit armé international en soi. Cette question, qui excède le cadre de cet article, a été étudiée par les auteurs du *Manuel Tallinn*. Voir généralement Schmitt, *Tallinn Manual*, *supra* note 19 aux pp 79–84 (voir la règle 22 et les commentaires).

Dans le cadre de cet article, nous appelons « cyberattaque étatique » toute cyberattaque parrainée[39] ou lancée directement par un État A[40] ou pour son compte[41], à son instigation[42] ou en raison de sa passivité délibérée[43], à partir du territoire dudit État contre un environnement informatique ou une infrastructure située sur le territoire d'un État B[44]. Les auteurs de cyberattaques étatiques peuvent être des agents *de jure* ou de *facto* de l'État[45]. Toutefois, « [s]i nombre de pays, à l'image des États-Unis, reconnaissent ouvertement développer des capacités offensives dans le domaine informatique, aucune attaque informatique n'a jusqu'à présent été publiquement revendiquée par un État »[46]. Au cours des dix dernières années, il a été souvent constaté que nombre de cyberattaques étatiques[47] étaient le fait de groupes d'individus aux motivations diverses agissant (prétendument) à la solde d'un État[48] ou de leur propre initiative[49] sans que leurs actions illicites contre un autre État ne soient dénoncées par le pays d'où sont lancées les attaques[50]. Les individus et entités impliqués dans des cyberattaques contre d'autres États le

39 Voir par ex Noah Schachtman, « Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It », *The Wired* (11 mars 2009), en ligne : <www.wired.com/2009/03/georgia-blames/> [Schachtman]. Voir aussi Canada, *Stratégie de cybersécurité*, *supra* note 16 à la p 5.

40 Voir par ex « Pentagon: Chinese government waging cyberattacks », *CBS News* (6 mai 2013), en ligne : <www.cbsnews.com/news/pentagon-chinese-government-waging-cyberattacks/> ; Gopal Ratnam, « Pentagon Accuses China of Cyberspying on U.S. Government », *Bloomberg* (7 mai 2013), en ligne : <www.bloomberg.com/news/print/2013-05-06/china-s-military-ambitions-growing-pentagon-report-finds.html>. Voir toutefois France, *Rapport d'information du Sénat*, *supra* note 3 (« [l]es autorités de Pékin ont toujours démenti ces accusations en mettant en avant le fait que la Chine serait elle aussi une victime » [emphase omise]) à la p 37. Voir aussi Carr, *Inside Cyber*, *supra* note 19 à la p 161 (sur le rôle de la Russie dans le lancement de cyberattaques contre d'autres pays).

41 Voir Geers et al, *supra* note 34 à la p 4.

42 Voir par ex Gardham, *supra* note 11.

43 Voir notamment Carr, *Inside Cyber*, *supra* note 19 à la p 161. Voir par ex « Estonia hit », *BBC News*, *supra* note 35.

44 Voir toutefois Schmitt, *Tallinn Manual*, *supra* note 19 (voir la règle 30 où l'on note qu'une cyber-attaque est « [u]ne cyberopération, offensive ou défensive, dont on s'attend raisonnablement à ce qu'elle cause des lésions ou la mort de personnes ou des dommages ou la destruction d'objets » [notre traduction] à la p 106).

45 Christian Czosseck, « State Actors and their Proxies in Cyberspace » dans Ziolkowski, *Peacetime Regime*, *supra* note 7, 1 aux pp 12–15 ; Carr, *Inside Cyber*, *supra* note 19 à la p 2 (Opération israélienne *Cast Lead* contre la Palestine). Voir aussi Matt Gurney, « Matt Gurney: In his secret war against Iran, Obama sends in the geeks », *National Post* (1 juin 2012), en ligne : <news.nationalpost.com/2012/06/01/matt-gurney-in-his-secret-war-against-iran-obama-sends-in-the-geeks/> [Gurney] ; « The mouse that roared: Is cyberwarfare a serious threat? », *The Economist* (5 septembre 2007), en ligne : <www.economist.com/node/9752625/print>.

46 France, *Rapport d'information du Sénat*, *supra* note 3 à la p 36.

47 Carr, *Inside Cyber*, *supra* note 19 aux pp 15–29, 89–102. Voir aussi Schreier, *supra* note 17 aux pp 107–115.

48 Voir Carr, *Inside Cyber*, *supra* note 19 à la p 117. Voir par ex Gardham, *supra* note 11 ; Tania Branigan et Kevin Anderson, « Google attacks traced back to China, says US internet security firm », *The Guardian* (14 janvier 2010), en ligne : <www.theguardian.com/technology/2010/jan/14/google-attacks-traced-china-verisign>.

49 France, *Rapport d'information du Sénat*, *supra* note 3 à la p 33.

50 Voir Carr, *Inside Cyber*, *supra* note 19 à la p 3. Voir par ex Charles Clover, « Kremlin-backed group behind Estonia cyber blitz », *Financial Times* (11 mars 2009), en ligne : <www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz3QSFVOS14> [Clover].

font souvent pour des raisons essentiellement patriotiques, les attaques étant alors effectuées dans un souci de revendication ou de protestation[51] contre les décisions politiques d'un autre État[52].

B. Quelques méthodes et moyens de commission des cyberattaques étatiques

L'analyse des outils utilisés pour le lancement d'attaques informatiques permet d'en faire ressortir l'ingéniosité et la furtivité, ce qui rend aisée l'évaluation des défis posés par ces nouvelles armes. Les deux méthodes qui ont été les plus utilisées depuis 2006 pour exécuter des cyberattaques étatiques sont : l'infection de réseaux par des programmes malveillants et les attaques de sites internet[53].

1. *L'installation clandestine de logiciels malveillants*[54]

Un logiciel malveillant est un programme informatique infiltré dans un réseau, à l'insu de son propriétaire ou de son utilisateur, avec l'intention de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications de la victime ou du système d'exploitation ; ou uniquement dans le but d'importuner la victime[55]. Il peut se présenter sous la forme d'un virus[56], d'un ver[57] ou d'un cheval de Troie[58]. L'intégrité d'un réseau informatique peut aussi être compromise

51 France, *Rapport d'information du Sénat*, *supra* note 3 à la p 33.

52 Voir par ex Kadri Kaska, Anna-Maria Talihärm et Eneken Tikk, « Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007 » dans Eneken Tikk et Anna-Maria Talihärm, dir, *International Cyber Security Legal and Policy Proceedings*, Tallinn (Estonie), Cooperative Cyber Defence Centre of Excellence Publications, 2010, 40 à la p 46 [Kaska, Talihärm et Tikk, « Developments in Estonia »] ; Clover, *supra* note 50.

53 Voir par ex James Andrew Lewis, « Significant Cyber Incidents Since 2006 », en ligne : (2014) Center for Strategic & International Studies <csis.org/files/publication/140807_Significant_Cyber_Incidents_Since_2006.pdf> ; Eneken Tikk, Kadri Kaska et Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn (Estonie), Cooperative Cyber Defence Centre of Excellence, 2010 [Tikk, Kaska et Vihul, *Cyber*] ; France, *Rapport d'information du Sénat*, *supra* note 3 (« [les] attaques de saturation par déni de service, le vol ou l'altération de données grâce à un logiciel malveillant et la destruction d'un système par un virus informatique constituent trois types d'attaques informatiques largement utilisées aujourd'hui ») à la p 26. Voir aussi Schreier, *supra* note 17 aux pp 107–15.

54 Nous nous contenterons de décrire très sommairement les caractéristiques principales des différents logiciels malveillants les plus utilisés.

55 Kissel, *Glossary*, *supra* note 16 à la p 115.

56 Un tel programme peut corrompre ou effacer des données dans un disque dur. Il s'agit d'un programme malveillant qui se réplique tout seul et se dissémine dans un ordinateur en affectant d'autres fichiers et d'autres programmes légitimes appelés hôtes (voir *ibid* à la p 205).

57 Il a les mêmes effets néfastes qu'un virus mais des méthodes de transmission différentes. C'est un programme qui se réplique tout seul et qui se transmet au moyen d'outils de communication de large portée tels qu'Internet ou un réseau d'entreprise. Un ver peut affecter plusieurs ordinateurs et contrairement à un virus, n'a pas besoin d'un programme hôte pour fonctionner (voir *ibid* à la p 208).

58 C'est un programme d'apparence légitime qui comporte en plus des fonctions déclarées, un mécanisme caché qui s'exécute en même temps que les actions connues de l'utilisateur (voir généralement Robert Longeon et Jean-Luc Archimbaud, « Guide de la sécurité des systèmes d'information à

à l'aide d'un logiciel espion qui est un programme conçu afin de récolter, à leur insu, de l'information sur les utilisateurs ou les organisations propriétaires du réseau infecté[59]. Ces informations sur l'environnement sont ensuite transmises à des personnes non autorisées[60]. La bombe logique est un autre type de logiciel malveillant, à mode de déclenchement différé et conçu pour causer des dommages à un système informatique ou exécuter certaines actions, uniquement lorsque certaines conditions prédéfinies par le créateur du programme sont réunies[61].

2. *Les attaques cybernétiques contre des sites internet*

Le déni de service, encore appelé attaque par saturation, a pour objectif le blocage de l'accès autorisé à des réseaux, des systèmes ou des applications, en envoyant simultanément un grand nombre de requêtes de connexion, ce qui finit par provoquer une déperdition des ressources informatiques[62]. Ce type d'attaque cherche à perturber le bon fonctionnement d'un service, le plus souvent celui d'un site internet. Le déni de service fait partie des cyberattaques dont les effets sont immédiatement apparents et les plus incommodants. Bien que les sites internet affectés se retrouvent bloqués, leur contenu n'est pas affecté pour autant, à moins que les dénis ne soient accompagnés d'actes de défiguration des pages[63]. Lorsque l'attaque est commise à l'aide de plusieurs ordinateurs, on parle de déni de service distribué[64]. Les dénis de service distribués sont très faciles à mettre en place et difficiles à interrompre.

Les cyberattaques présentent de nouveaux défis en matière de relations internationales. Leurs conséquences peuvent aller du brouillage de signaux numériques de communication à la perturbation, voire la neutralisation des infrastructures critiques d'un État, ce qui est en mesure de provoquer la panique au sein de la population et des dommages aussi bien humains que matériels[65].

---

l'usage des directeurs » (1999) 2e trimestre, Centre national de la recherche scientifique à la p 66 [Longeon et Archimbaud]). Voir aussi Kissel, *Glossary*, *supra* note 16 à la p 196 (en général, le but d'un cheval de Troie est de créer une « porte dérobée » afin qu'un pirate informatique puisse avoir un accès ultérieur aisé à l'ordinateur ou au réseau informatique. L'administrateur du réseau ou l'utilisateur de l'ordinateur ayant perdu le contrôle de celui-ci, le pirate peut alors recueillir, détruire des données ou exécuter d'autres actions nuisibles à l'intégrité du système). Voir par ex Gellman et Nakashima, « U.S. spy », *supra* note 11.

59 Kissel, *Glossary*, *supra* note 16 à la p 182.

60 *Ibid*.

61 Longeon et Archimbaud, *supra* note 58.

62 Kissel, *Glossary*, *supra* note 16 à la p 61. Voir notamment Jennifer A Chandler, « Security in Cyberspace: Combatting Distributed Denial of Service Attacks » (2003-04) 1:1-2 Rdr & technologie de U Ottawa 231.

63 France, *Rapport d'information du Sénat*, *supra* note 3 à la p 155 (il s'agit de la violation de l'intégrité des pages d'un site internet par l'altération de leur apparence ou du contenu du serveur internet).

64 Kissel, *Glossary*, *supra* note 16 à la p 64.

65 Papanastasiou Afroditi, « Application of International Law in Cyber Warfare Operations » (8 septembre 2010), en ligne : <ssrn.com/abstract=1673785> à la p 9.

III. LE 21E SIÈCLE, L'ÈRE DES CONFLITS INTERÉTATIQUES NUMÉRIQUES : QUELQUES EXEMPLES DE CYBERATTAQUES ÉTATIQUES

En 1999, dans son livre précurseur sur le cyberespace et l'emploi de la force, Sharp affirmait que l'espionnage et les attaques informatiques étaient parmi les questions les plus urgentes auxquelles devraient faire face les États sur la scène internationale[66]. Une décennie à peine plus tard, les manchettes de la presse internationale semblent lui avoir donné raison[67].

A. Internet, le talon d'Achille de l'Estonie

Le 26 avril 2007, le gouvernement estonien fait déplacer, un monument de la Seconde Guerre mondiale dédié à la mémoire de l'Armée rouge, du centre-ville de Tallinn vers un cimetière militaire à l'extérieur de celle-ci. La communauté russophone estonienne, qui représente près de 30 % de la population, ainsi que la Russie, émettent de vives protestations contre la décision du gouvernement estonien, les premiers par des manifestations populaires, les seconds par des déclarations publiques[68]. Le lendemain des manifestations, et ce, pendant plus de trois semaines, une série de dénis distribués de service paralysent plusieurs sites internet gouvernementaux et privés estoniens, notamment ceux des médias[69], des banques, des opérateurs de téléphonie mobile et des services d'urgence[70]. Les perturbations informatiques atteignent leur apogée le 9 mai[71], date à laquelle la fin de la Seconde Guerre mondiale est commémorée en Russie. Les attaques sont aussi accompagnées de défigurations de sites internet et d'envoi massif de pourriels[72]. Le caractère soudain et coordonné des attaques ainsi que leur envergure font penser à une implication étatique[73]. Si ces dénis de service ne résultent en aucune destruction matérielle, « elles [perturbent] de manière spectaculaire le fonctionnement de la

---

66 Sharp, *supra* note 36 à la p 123.

67 Voir par ex McCurry, *supra* note 11 ; Nakashima, « Cyberattacks », *supra* note 12 ; « US looking », *The Sydney Morning Herald*, *supra* note 12 ; Sanger, « In Cyberspace », *supra* note 13.

68 Voir par ex « One Killed In Estonian Violence Over War Memorial », *Radio Free Europe Radio Liberty* (27 avril 2007), en ligne : <www.rferl.org/content/article/1076138.html> [« One Killed », *RFERL*] ; « Putin Warns Against "Belittling" War Effort », *Radio Free Europe Radio Liberty* (9 mai 2007), en ligne : <www.rferl.org/content/article/1076356.html> ; « Estonia hit », *BBC News*, *supra* note 35.

69 Voir par ex Traynor, « Russia accused », *supra* note 35.

70 Voir par ex Arthur Bright, « Estonia accuses Russia of "cyberattack" », *The Christian Science Monitor* (17 mai 2007), en ligne : <www.csmonitor.com/layout/set/print/2007/0517/p99s01-duts.html> [Bright] ; « Cyberwarfare: Newly nasty », *The Economist* (24 mai 2007), en ligne : <www.economist.com/node/9228757>.

71 Jose Nazario, « Politically Motivated Denial of Service Attacks » dans Christian Czosseck et Kenneth Geers, dir, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam (Pays-Bas), IOS Press, 2009, 163 [Nazario, « Politically Motivated DoS »].

72 Kaska, Talihärm et Tikk, « Developments in Estonia », *supra* note 52 à la p 45.

73 *Ibid* à la p 44.

vie courante du pays, en privant les usagers de l'accès à certains services en ligne essentiels » [emphases omises][74].

Durant les premières heures des attaques contre les sites internet estoniens, les sources de celles-ci sont identifiées, par Tallinn, comme étant des ordinateurs appartenant à des groupes nationalistes russes[75] ainsi qu'à des institutions gouvernementales russes[76]. La Russie dément toute implication[77]. Par la suite, les attaques sont reliées à des ordinateurs se trouvant dans 178 pays[78]. L'Estonie admet, par la suite en septembre 2007, ne pas pouvoir affirmer sans aucun doute que Moscou est effectivement responsable des attaques dont elle a été victime[79].

En mars 2009, lors d'un panel de discussion sur les guerres d'information au 21e siècle, un député de la Douma déclare que les attaques contre l'Estonie avaient été lancées par son assistant, de la propre initiative de ce dernier[80]. Quelques jours plus tard, un groupe de jeunes patriotes russes, *Nashi*[81], endosse la responsabilité desdites attaques[82]. *Nashi* est un mouvement de jeunesse russe proche du Kremlin et subventionné par celui-ci[83] qui avait établi des piquets de protestation devant l'ambassade estonienne à Moscou au début de la crise russo-estonienne de 2007, décrivant leur action comme étant un « blocus » de la représentation diplomatique[84].

---

74 France, *Rapport d'information du Sénat*, *supra*, note 3 à la p 12.

75 Voir Sheng Li, « When Does Internet Denial Trigger the Right of Armed Self-Defense? » (2013) 38:1 Yale J Intl L 179 à la p 180. Voir par ex « Estonia hit », *BBC News*, *supra* note 35.

76 Voir notamment Republic of Estonia Government, communiqué, « Declaration of the Minister of Foreign Affairs of the Republic of Estonia » (1 mai 2007), en ligne : <https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia> [Estonia, « Declaration of the MFA »]. Voir par ex Traynor, « Russia accused », *supra* note 35 ; Bright, *supra* note 70 ; Steven Lee Myers, « "E-stonia" Accuses Russia of Computer Attacks », *The New York Times* (18 mai 2007), en ligne : <www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h> [Myers].

77 Traynor, « Russia accused », *supra* note 35 ; « Kremlin brushes off Estonian accusations of hacker attacks », *Ria Novosti* (17 mai 2007), en ligne : <en.rian.ru/russia/20070517/65661919.html> [« Kremlin », *Ria Novosti*].

78 Tikk, Kaska et Vihul, *Cyber*, *supra* note 53 à la p 23. Voir aussi Myers, *supra* note 76.

79 « Estonia has no evidence of Kremlin involvement in cyber attacks », *Ria Novosti* (6 septembre 2007), en ligne : <en.rian.ru/world/20070906/76959190.html> [« Estonia has no evidence », *Ria Novosti*].

80 Robert Coalson, « Behind The Estonia Cyberattacks », *Radio Free Europe Radio Liberty* (6 mars 2009), en ligne : <www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html>.

81 James Rodgers, « Putin's next generation make their mark », *BBC News* (4 mai 2007), en ligne : <news.bbc.co.uk/2/hi/europe/6624549.stm>.

82 Kaska, Talihärm et Tikk, « Developments in Estonia », *supra* note 52. Voir aussi Clover, *supra* note 50.

83 Voir par ex Anselm Waldermann, « The Nashi Movement: Russian Youth and the Putin Cult », *Spiegel Online* (11 février 2007), en ligne : <www.spiegel.de/international/world/the-nashi-movement-russian-youth-and-the-putin-cult-a-514891-druck.html> ; James Jones, « Putin's youth movement provides a sinister backdrop to Russia's protests », *The Guardian* (8 décembre 2011), en ligne : <www.theguardian.com/commentisfree/2011/dec/08/putin-russia-elections> ; Miriam Elder, « Polishing Putin: hacked emails suggest dirty tricks by Russian youth group », *The Guardian* (7 février 2012), en ligne : <www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi>.

84 Voir notamment Estonia, « Declaration of the MFA », *supra* note 76 ; René Värk, « The Siege of the Estonian Embassy in Moscow: Protection of a Diplomatic Mission and Its Staff in the Receiving State » (2008) 15 Juridica International 144 à la p152 ; « One Killed », *RFERL*, *supra* note 68.

B. Le conflit russo-géorgien, premier cyberconflit international ?

Sur fond de divergences politicomilitaires avec la Russie au sujet du statut de l'Abkhazie et de l'Ossétie du Sud, la Géorgie est victime d'attaques informatiques provenant de ce pays pendant l'été 2008[85]. Du 19 au 20 juillet 2008, le site internet du président géorgien subit une attaque massive par déni de service contenant le message de propagande politique prorusse suivant : « Win+love+in+Russia »[86]. C'est ensuite le calme plat jusqu'au 7 août[87], date officielle du début du conflit armé international entre la Géorgie et la Fédération russe[88]. Quelques heures avant[89] le

85 Schachtman, *supra* note 39 ; John Markoff, « Georgia Takes a Beating in the Cyberwar With Russia », *The New York Times* (11 août 2008), en ligne : <bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/> [Markoff, « Georgia Takes »] ; Ron Synovitz, « Georgian Government Accuses Russia Of Waging "Cyberwarfare" », *Radio Free Europe Radio Liberty* (12 août 2008), en ligne : <www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html> [Synovitz].

86 Voir notamment CE, *Independent International Fact-Finding Mission on the Conflict in Georgia* (2009) vol II à la p 218 [CE, *Independent Mission in Georgia* vol II] ; Eneken Tikk et al, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Tallin (Estonie), Cooperative Cyber Defence Centre of Excellence, 2008 à la p 5 [Tikk et al, *Georgia: Legal Lessons*] ; Nazario, « Politically Motivated DoS », *supra* note 71 ; Jose Nazario et Andre M DiMino, « An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008 », *Arbor Networks et Shadowserver*, en ligne : <https://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf> à la p 11 [Nazario et DiMino] ; Dancho Danchev, « Georgia President's web site under DDoS attack from Russian hackers » (22 juillet 2008), ZDNet (blogue), en ligne : <www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533> ; Steven Adair, « The Website for the President of Georgia Under Attack - Politically Motivated? », *Shawdowserver* (19 juillet 2008), en ligne : <https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720>. Voir aussi Jon Swaine, « Georgia: Russia "conducting cyber war" », *The Telegraph* 11 (août 2008), en ligne : <www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> ; John Markoff, « Before the Gunfire, Cyberattacks », *The New York Times* (12 août 2008), en ligne : <www.nytimes.com/2008/08/13/technology/13cyber.html?ref=europe&_r=1&> [Markoff, « Before the Gunfire »].

87 Voir notamment CE, *Independent Mission in Georgia* vol II, *supra* note 86 à la p 218 ; Tikk et al, *Georgia: Legal Lessons*, *supra* note 86 à la p 4 ; US Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 2009, en ligne : <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf> à la p 2 [US-CCU]. Voir aussi Jeffrey Carr et al, « Russia/Georgia Cyber War – Findings and Analysis », en ligne : (2008) *Project Grey Goose: Phase I Report* à la p 8 <fr.scribd.com/doc/6967393/Project-Grey-Good-Phase-I-Report#scribd> (le *Project Grey Goose* est un projet informatique mis en place après les cyber-attaques, dans le seul but de déterminer si le gouvernement russe était impliqué dans celles-ci ou si les dénis de service relevaient uniquement d'initiatives patriotiques de pirates informatiques russes).

88 Voir notamment CE, *Independent International Fact-Finding Mission on the Conflict in Georgia* (2009) vol I à la p 19 (selon les informations fournies par le gouvernement géorgien, le président géorgien a donné l'ordre de commencer une opération défensive le 7 août à 23 h 35) [CE, *Independent Mission in Georgia* vol I] ; « Article 2(4) » dans *Répertoire de la pratique suivie par les organes des Nations Unies*, vol 1, supp n° 10, NU, 2000-09 au para 15.

89 Voir notamment Tikk et al, *Georgia: Legal Lessons*, *supra* note 86 aux pp 4–5 ; US-CCU, *supra* note 87 à la p 6. Voir aussi David Hollis, « Cyberwar Case Study: Georgia 2008 », en ligne : (2011) Small Wars Journal à la p 3 <smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008> [Hollis].

début de l'invasion terrestre de la Géorgie par l'armée russe[90], le trafic internet au départ et à destination de la Géorgie est redirigé vers la Russie et la Turquie où il est ensuite bloqué[91]. La Géorgie se retrouve coupée du reste du monde en ce qui concerne Internet : ni les personnes vivant en Géorgie, ni celles se trouvant à l'extérieur de celle-ci, ne peuvent être informées des récents développements militaires[92]. Le 8 août, Tbilissi accuse Moscou d'avoir eu recours à des pirates informatiques pour exécuter des cyberattaques contre des sites internet géorgiens, gouvernementaux et d'information[93], la Russie réfutant ces accusations[94]. Il est important de faire remarquer qu'au cours des semaines qui ont suivi la cyberattaque de juillet 2008 et ont précédé celle du 7 août 2008, plusieurs discussions à connotation patriotique, sur l'opportunité de recourir à des dénis de service, accompagnés cette fois-ci de défigurations de site internet, ont eu lieu entre les usagers de différents forums internet russes[95]. À partir du 9 août 2008, des sites et des forums de discussions sont spécialement créés sur Internet par des groupes russes[96] d'individus aux motivations apparemment nationalistes[97], qui organisent et coordonnent les attaques par saturation dont sont victimes les sites géorgiens[98]. Des pirates informatiques sont ainsi recrutés, grâce à la mise à disposition en ligne d'instructions sur le mode de lancement de dénis de service et la fourniture de sites géorgiens à attaquer[99]. Il a été avancé que des organisations criminelles russes

---

90 CE, *Independent Mission in Georgia* vol I, *supra* note 88 à la p 20 (le début du conflit armé international est fixé officiellement le 7 août 2008 à 23 h 35, heure à laquelle le président géorgien a donné l'ordre à son armé d'amorcer une offensive militaire en Ossétie du Sud, cependant la Russie affirme que la première échange de feu entre ses forces armées et celles de la Géorgie a eu lieu le 8 août à 14 h 30). Voir aussi Hollis, *supra* note 89 à la p 1.

91 CE, *Independent Mission in Georgia* vol II, *supra* note 86 à la p 218. Voir aussi Markoff, « Georgia Takes », *supra* note 85 ; Synovitz, *supra* note 85.

92 Voir notamment US-CCU, *supra* note 87 à la p 5. En accord avec CE, *Independent Mission in Georgia* vol II, *supra* note 86 à la p 218 (tous les sites géorgiens sont inaccessibles des États-Unis, du Royaume-Uni et du cyberespace européen). Voir aussi Collin S Allan, « Attribution Issues in Cyberspace » (2013) 13:2 Chicago-Kent J Intl & Comp L 55 à la p 57 [Allan].

93 Voir Schachtman, *supra* note 39.

94 Voir par ex Synovitz, *supra* note 85.

95 Voir Steven Adair, « Georgian Attacks: Remember Estonia?: Georgia and Estonia Have Something New in Common », *Shadowserver Foundation* (13 août 2008), en ligne : <https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080813> [Adair, « Georgian Attacks »] ; Dancho Danchev, « Coordinated Russia vs Georgia cyber attack in progress » (11 août 2008), *ZDNet* (blogue), en ligne : <www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670> [Danchev]. Voir aussi Captain Paulo Shakarian, « The 2008 Russian Cyber Campaign Against Georgia » (2011) Military Rev 63 à la p 65 (déclaration du Colonel Anatoly Tsyganok, chef du centre russe de prévision militaire, qui décrit la cybercampagne « comme faisant partie d'une bataille plus importante par l'information » (*part of a larger information battle*) menée contre les médias géorgiens et occidentaux [notre traduction]).

96 Adair, « Georgian Attacks », *supra* note 95.

97 Nazario et DiMino, *supra* note 86 à la p 27.

98 Carr, *Inside Cyber*, *supra* note 19 aux pp 15, 106, 141.

99 US-CCU, *supra* note 87 aux pp 3, 5 ; Tikk et al, *Georgia: Legal Lessons*, *supra* note 86 aux pp 7–10. Voir aussi Kaska, Talihärm et Tikk, « Developments in Estonia », *supra* note 52 à la p 45 (ce fût aussi le cas pendant la campagne estonienne). Voir aussi Adair, « Georgian Attacks », *supra* note 95.

ont participé aux cyberattaques dont a été victime la Géorgie[100], certaines des adresses numériques incriminées ayant déjà été utilisées auparavant par le Russian Business Network (RBN), une organisation russe dissoute au moment des attaques et qui était impliquée dans la cybercriminalité[101]. Les autorités géorgiennes font alors héberger la plupart de leurs sites dans d'autres pays tels que les États-Unis, l'Estonie et la Pologne[102]. En dépit de ces mesures, tout au long du conflit armé qui oppose la Russie à la Géorgie, les sites internet géorgiens restent les cibles de dénis de service distribués accompagnés de défigurations contenant des messages de propagande politique prorusse[103]. Les attaques prennent fin peu de temps après le retrait des troupes russes de la Géorgie.

C. Stuxnet, une arme de guerre informatique de précision en temps de paix

Stuxnet est un ver qui ferait partie d'un programme secret américain intitulé *Olympic Games*[104]. Autorisé en 2006 par le président Georges Bush[105] et poursuivi par le président Barack Obama après sa prise de pouvoir en 2009[106], *Olympic Games* a pour objectif le sabotage du programme nucléaire iranien[107]. Bien qu'il eût été découvert pour la première fois en juin 2010[108], il est avancé que le ver était déjà en circulation avant cette date[109]. Conçue spécifiquement pour endommager les centrifugeuses du programme nucléaire iranien en modifiant leur vitesse de rotation[110], l'attaque par Stuxnet s'est déroulée en deux phases : les sites nucléaires iraniens ont été d'abord infiltrés par Duqu, un logiciel espion[111] qui retransmettait les plans des

---

100 US-CCU, *supra* note 87 à la p 3.

101 *Ibid* ; Tikk, Kaska et Vihul, *Cyber*, *supra* note 53 aux pp 74–75. Voir aussi Allan, *supra* note 92 à la p 58. *Contra* Mike Johnson, « Georgian Websites Under Attack - Don't Believe the Hype », *Shadowserver Foundation* (12 août 2008), en ligne : <https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080812>.

102 CE, *Independent Mission in Georgia* vol II, *supra* note 86 à la p 217. Voir aussi Danchev, *supra* note 95. Comparer Ophardt, *supra* note 6 au para 27 (même après le déménagement des serveurs de certains sites à l'extérieur de la Géorgie, les attaques ont continué, car c'était la Géorgie qui était attaquée dans le cyberespace, et non un simple site internet).

103 US-CCU, *supra* note 87 à la p 6.

104 David E Sanger, « Obama Order Sped Up Wave of Cyberattacks Against Iran », *The New York Times* (1 juin 2012), en ligne : <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=al> [Sanger, « Obama Order »].

105 Gurney, *supra* note 45.

106 Sanger, « Obama Order », *supra* note 104.

107 David E Sanger, « U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site », *The New York Times* (10 janvier 2009), en ligne : <www.nytimes.com/2009/01/11/washington/11iran.html?> ; Gurney, *supra* note 45.

108 Jonathan Fildes, « Stuxnet worm "targeted high-value Iranian assets" », *BBC News* (23 septembre 2010), en ligne : <www.bbc.co.uk/news/technology-11388018> [Fildes] ; Gurney, *supra* note 45.

109 Fildes, *supra* note 108.

110 *Ibid*.

111 Nicole Perlroth, « Researchers Find Clues in Malware », *The New York Times* (30 mai 2012), en ligne : <www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html>.

centrales nucléaires iraniennes aux services de renseignements américains[112]. Ces plans ont servi plus tard à la mise en place des tests de qualité de Stuxnet avant son déploiement[113]. La seconde étape a constitué en l'infection des contrôleurs des centrifugeuses par le ver Stuxnet. Stuxnet est aussi une bombe logique qui est censée être inactive si elle ne reconnaît pas sa cible ; le ver est, par la suite, supposé s'autodétruire, une fois sa tâche de dégradation des Systèmes de traitement automatisé des données (ci-après « STAD »)[114] accomplie[115]. Les systèmes de détection d'incidents des centrifugeuses ont aussi été modifiés par Stuxnet ; en effet, ces derniers semblaient fonctionner normalement aux yeux des ingénieurs iraniens alors qu'elles étaient en train de s'user, tournant parfois trop rapidement ou trop lentement selon les commandes envoyées par le ver[116]. À la suite d'une erreur de manipulation[117], Stuxnet s'est diffusé sur le réseau Internet : c'est ainsi que son existence a été révélée au monde entier.

En novembre 2010, les autorités iraniennes annoncent que des centrifugeuses du programme iranien nucléaire ont été infectées par un ver informatique[118] et accusent les États-Unis d'être à l'origine de l'attaque[119]. Après des séries d'entretiens sous couvert d'anonymat d'une durée de 18 mois, avec des responsables américains et israéliens, le journaliste américain David E Sanger révèle que Stuxnet aurait été créé par les services de renseignement américains et israéliens[120]. Les États-Unis n'ont ni confirmé ni nié leur implication dans la création de Stuxnet ; cependant, une enquête a été lancée pour découvrir l'origine des fuites[121].

---

112 Christopher Williams, « Barack Obama "ordered Stuxnet cyber attack on Iran" », *The Telegraph* (1 juin 2012), en ligne : <www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html> [Williams].

113 William J Broad, John Markoff et David E Sanger, « Israeli Test on Worm Called Crucial in Iran Nuclear Delay », *The New York Times* (15 janvier 2011), en ligne : <www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>[Broad, Markoff et Sanger].

114 Habituellement désignés par leur acronyme anglais SCADA (*supervisory, control and data acquisition*).

115 Barbara Louis-Sidney, « La dimension juridique du cyberespace » (2012-13) 87 R Intl & stratégique 73 à la p 74 [Louis-Sidney] ; Andrew C Foltz, « Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate » (2012) 67:4 Joint Force Q 40 à la p 44.

116 Gurney, *supra* note 45 ; « US unleashed Stuxnet cyber war on Iran to appease Israel – report », *RT* (1 juin 2012), en ligne : <www.rt.com/news/iran-us-israel-cyberwar-virus-weapon-770/> [« US unleashed », *RT*].

117 Voir notamment Sanger, « Obama Order », *supra* note 104. Voir aussi Fildes, *supra* note 108 ; Gurney, *supra* note 45 ; Williams, *supra* note 112 ; « US unleashed », *RT*, *supra* note 116.

118 Broad, Markoff et Sanger, *supra* note 113.

119 « Iran's nuclear negotiator says U.S. involved in cyberattack », *NBC News* (17 janvier 2011), en ligne : <www.nbcnews.com/id/41121090/ns/world_news-mideastn_africa>.

120 Voir notamment Sanger, « Obama Order », *supra* note 104. Voir généralement Broad, Markoff et Sanger, *supra* note 113. Voir aussi JTA, « Snowden says Israel, U.S. created Stuxnet virus that attacked Iran », *Haaretz* (9 juillet 2013), en ligne : <www.haaretz.com/news/diplomacy-defense/1.534728>.

121 Evan Perez et Adam Entous, « FBI Probes Leaks on Iran Cyberattack », *The Wall Street Journal* (5 juin 2012), en ligne : <online.wsj.com/article/SB10001424052702303506404577448563517340188.html> [Perez et Entous] ; « Former US general James Cartwright named in Stuxnet leak inquiry », *The Guardian* (28 juin 2013), en ligne : <www.guardian.co.uk/world/2013/jun/28/general-cartwright-investigated-stuxnet-leak>.

IV. LES ENJEUX POSÉS PAR LES CYBERATTAQUES ÉTATIQUES DANS LES RELATIONS INTERNATIONALES

Les cyberattaques étatiques remettent en cause les notions traditionnelles de frontières puisqu'elles sont conduites dans le cyberespace, un environnement caractérisé par son « anonymat » et son « ubiquité » [notre traduction][122], ce qui rend l'attribution des attaques extrêmement difficile.

A. La nébulosité des cyberattaques étatiques

« L'information est la denrée prisée du cyberespace » [notre traduction][123] et l'arme informatique, en raison de son caractère clandestin, protéiforme et rapide, représente le moyen parfait de l'obtenir, toute lapalissade mise de côté. « Agir discrètement, anonymement, subrepticement, dans l'objectif, entre autre[s], de gagner du temps et de développer, ou de préserver des capacités de lutte informatique clandestines, parfois à des fins de sabotage ou d'espionnage »[124], telle est la raison d'être des cyberattaques.

1. *Les obstacles techniques à l'attribution des cyberattaques*

Les auteurs de cyberattaques utilisent plusieurs méthodes de camouflage telles que l'infiltration de logiciels malveillants par le biais d'Internet et le recours à des techniques d'usurpation d'adresse internet ou la prise de contrôle à distance, à l'insu de leurs propriétaires, d'ordinateurs hôtes qui seront utilisés pour lancer les attaques. Par exemple, la localisation dans un pays donné du serveur ayant permis le lancement d'une cyberattaque ne veut pas forcément dire que les auteurs de l'attaque se trouvent dans cet État et encore moins que ce pays est à l'origine de l'attaque[125]. Les difficultés d'attribution font qu'il est difficile pour un État victime d'une cyberattaque d'agir contre les auteurs pendant, mais aussi après, l'attaque.

---

122 von Heinegg, *supra* note 16 à la p 9. Voir généralement Schreier, *supra* note 17 aux pp 93–106.

123 Sharp, *supra* note 36 à la p 15.

124 Louis-Sidney, *supra* note 115 à la p 81. Voir aussi Nicholas Tsagourias, « The prohibition of threats of force » (2012) 17:2 J Confl & Sec L 229 à la p 233.

125 Il est aussi possible pour des pirates informatiques basés dans un pays A de prendre le contrôle d'ordinateurs situés dans un pays B pour lancer des attaques contre le réseau informatique d'un pays C. Voir par ex The Associated Press, « Cyberattack hits South Korean banks, TV networks », *CBC News* (20 mars 2013), en ligne : <www.cbc.ca/news/world/cyberattack-hits-south-korean-banks-tv-networks-1.1363815> ; AP, « Chinese internet », *supra* note 11. Voir aussi Cornish et al, *supra* note 34 à la p 13.

2. *Des opérations sans liens étatiques probants*

Si l'on se fie uniquement aux démentis publics ou au silence des États, il n'y a jamais eu à ce jour de cyberattaque étatique[126]. La particularité de ces opérations est qu'elles sont conduites en secret et ne sont pas admises publiquement comme faisant partie de la politique étrangère d'un État. En règle générale, même quand l'implication d'un État est révélée au grand jour, il n'admet jamais avoir effectué pareilles activités clandestines ou les avoir commanditées[127]. Par ailleurs, l'emploi par certains États d'agents privés pour la perpétration d'attaques informatiques à l'encontre d'un autre État, rend difficile la détermination d'une quelconque responsabilité internationale, du moins d'un point de vue juridique[128]. « Le problème, dans ces conditions, n'est pas l'opération juridique consistant à imputer le fait à un État déterminé aux fins d'établir sa responsabilité, mais l'opération préalable de recherche des preuves matérielles permettant d'en identifier l'auteur »[129]. Comment un État B dont les sites institutionnels sont paralysés après des dénis de service distribués, organisés par des pirates informatiques situés dans un État A, pourrait apporter la preuve judiciaire d'une implication de l'État A, sans la coopération dudit État ? En effet, en raison du « contrôle territorial exclusif exercé par l'État dans les limites de ses frontières […] l'État victime d'une violation du droit international se trouve souvent dans l'impossibilité de faire la preuve directe des faits d'où découlerait la responsabilité »[130]. Ce fut le cas pour l'Estonie. En mai 2007, aussitôt après les attaques informatiques qu'elle a subies, Tallinn soumet une demande de coopération pénale à la Russie en vertu d'un accord d'assistance bilatéral entre les deux pays en la manière, et ce, afin d'identifier les propriétaires de certaines adresses numériques russes impliquées dans les dénis de service[131]. La Russie rejette la demande en juin 2008 en indiquant que le traité invoqué ne s'appliquait pas dans la présente situation[132].

3. *Des attaques informatiques aux motifs et aux intentions souvent indiscernables*

Il est très rare que les cyberattaques de grande envergure soient commises sans raison aucune : ce sont souvent des moyens pour une fin déterminée d'avance par

126 Voir par ex Schachtman, *supra* note 39 ; « Estonia has no evidence », *Ria Novosti*, *supra* note 79 ; « Kremlin », *Ria Novosti*, *supra* note 77. Voir aussi France, *Rapport d'information du Sénat*, *supra* note 3 à la p 36 ; Perez et Entous, *supra* note 121.

127 Captain James A Burger, *Subversive Activities – An Area Within or Outside the Scope of International Law?*, thèse de maîtrise en droit, Judge Advocate General's School, United States Army, 1975 [non publiée] à la p 10.

128 Katharina Ziolkowski, « *Ius ad bellum* in Cyberspace: Some Thoughts on the "Schmitt-Criteria" for Use of Force » dans Czosseck, Ottis et Ziolkowski, *2012*, *supra* note 16, 295 à la p 306.

129 *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c États-Unis d'Amérique)*, [1986] CIJ rec 14 au para 57.

130 *Affaire du Détroit de Corfou*, [1949] CIJ rec 4 à la p 18.

131 Tikk, Kaska et Vihul, *Cyber*, *supra* note 53 à la p 27.

132 *Ibid*.

les auteurs[133]. Lorsqu'il s'agit d'attaques aux effets immédiats comme les dénis de service, il est assez facile de discerner les intentions de l'attaquant : causer des désagréments majeurs pour la victime. Cependant, à défaut de l'occurrence d'une cyberattaque aux effets dévastateurs, tangibles ou quantifiables, il est très difficile pour un État d'être certain de l'intention de l'auteur d'une intrusion informatique. En effet, tandis que, dans la vie réelle, l'intention permet de faire la distinction entre un acte d'hostilité étatique et un simple vol de reconnaissance aérienne[134], le caractère extrêmement clandestin des opérations informatiques menées dans le cyberespace rend difficile cette distinction. Lorsqu'une intrusion informatique est constatée, il est presque impossible de déterminer immédiatement avec certitude si l'on est en présence d'une simple activité de surveillance de réseau, de collecte d'informations, d'une opération en prélude à une attaque future ou d'une attaque en cours dont les effets ne se font pas encore sentir. Si l'on prend l'exemple de la cyberattaque dont a été victime le programme nucléaire iranien, l'infiltration du ver Stuxnet a été précédée du déploiement de la balise informatique Duqu[135]. Rien ne permet de garantir que la découverte de Duqu par les autorités iraniennes avant l'infection par Stuxnet leur aurait permis d'anticiper à quoi auraient servi les plans copiés, notamment si l'Iran ne savait pas qui était à l'origine de l'attaque informatique. Même si l'on peut avoir une idée des motivations derrière une attaque quelconque, les intentions ultimes d'un État sont particulièrement difficiles à discerner dans le cas de cyberattaques étatiques[136].

B. La vulnérabilité croissante des infrastructures critiques aux cyberattaques

Bien que menées dans le cyberespace, les cyberattaques peuvent produire des effets aussi bien cinétiques que non électroniques à l'extérieur du cyberespace, ceci pouvant être le but exact recherché par l'attaquant[137]. En effet, les réseaux d'infrastructures critiques[138] qui représentent l'ensemble des services si essentiels au fonctionnement de base d'une société que leur dérèglement pourrait perturber le fonctionnement de la société entière sont gérés par des STAD. Ces systèmes permettent une

133 Geers et al, *supra* note 34 à la p 2 ; Comparer Michael N Schmitt, « Wired warfare: Computer network attack and *jus in bello* » (2002) 84:846 RICR 365 à la p 373.

134 « Paragraphe 4 de l'article 2 », dans *Répertoire de la pratique suivie par les organes des Nations Unies*, vol 1, supp n° 3, NU, 1959-66 aux para 50–51 (le CSNU a considéré que le survol de l'espace aérien soviétique par un avion de reconnaissance américain ne constituait pas un acte d'agression, encore moins une violation de l'article 2(4), car cette reconnaissance n'avait pas été faite dans un but agressif ; l'avion n'était pas armé et surtout les États-Unis s'étaient engagés à ne plus recommencer).

135 Williams, *supra* note 112.

136 Sharp, *supra* note 36 à la p 127.

137 Melzer, « Cyberwarfare », *supra* note 16 à la p 5.

138 À ne pas confondre avec le terme informatique « infrastructure réseau » qui représente l'ensemble de serveurs, de câbles et de logiciels nécessaires à la connexion d'équipements informatiques à un réseau d'entreprise. Voir aussi *Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information*, Rés AG 58/199, Doc off AG NU, Doc NU A/RES/58/199, 58e sess, (2004) 1 à la p 1, aux para 2–3, 6.

surveillance et un contrôle globaux des réseaux d'approvisionnement, de transport et de distribution d'électricité, d'eau, de gaz, d'information et de communication ainsi que des services d'urgence et des les services bancaires et financiers. Les STAD peuvent être commandés à distance et donc être victimes de cyberattaques[139], comme l'a prouvé l'incident iranien. Il est difficile d'estimer les conséquences de telles attaques sur l'économie, la santé ou la sécurité publique d'un État, mais il ne fait aucun doute qu'une interruption simultanée des réseaux de distribution d'eau et d'électricité, couplée à une perturbation des services bancaires et financiers, sur toute l'étendue du territoire d'un pays pendant quelques heures, pourrait suffire à provoquer un vent de panique au sein de la population. Plus les services essentiels d'un pays sont contrôlés par une large infrastructure informatique, plus cet État est vulnérable à une cyberattaque pouvant résulter en des dommages considérables, équivalents sinon plus importants que ceux pouvant être commis par des armes plus classiques. Les cas estoniens[140] et géorgiens[141] l'ont d'ailleurs démontré, l'Estonie ayant été plus touchée que la Géorgie par les dénis de service que ces pays ont subis[142]. La multiplication de cyberattaques visant des structures étatiques a conduit plusieurs pays à faire de la cybersécurité une priorité nationale[143].

V. CONCLUSION

Dans un environnement international où l'arme nucléaire pousse les États à modérer leurs ardeurs belliqueuses, les cyberattaques offrent aux États une autre façon de s'affronter sans en avoir l'air[144], ce qui n'est pas sans rappeler les conflits de basse intensité de la Guerre froide[145]. Selon le département de défense américain, un conflit de basse intensité est une confrontation politicomilitaire entre des États ou des groupes concurrents, qui se situe au-dessous du seuil des guerres conventionnelles et qui est au-dessus de l'habituelle rivalité inoffensive que se livrent les États[146]. « Il est mené par une combinaison de moyens employant des instruments politiques,

---

139 *Ibid*.

140 Voir par ex « Estonia hit », *BBC News*, *supra* note 35 (le directeur de la sécurité informatique du ministère estonien de la défense a reconnu la vulnérabilité de son pays à des cyberattaques, usant même le « e-government » pour désigner le fonctionnement des institutions estoniennes).

141 Voir par ex Markoff, « Georgia Takes », *supra* note 85.

142 Ophardt, *supra* note 6 au para 10.

143 France, *Rapport d'information du Sénat*, *supra* note 3 (« [l]es États-Unis, le Royaume-Uni et l'Allemagne ont fait depuis déjà plusieurs années de la cybersécurité une priorité nationale et ont mis en place des dispositifs importants pour lutter contre les attaques informatiques ») à la p 38.

144 Waxman, « Cyber-Attacks », *supra* note 11 à la p 441 ; Morth, *supra* note 1 à la p 568. Voir par ex Sanger, « In Cyberspace », *supra* note 13 ; McCurry, *supra* note 11.

145 Samuel Liles, « Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency » dans C Czosseck et K Podins, dir, *Conference on Cyber Conflict Proceedings 2010*, Tallinn (Estonia), Cooperative Cyber Defence Centre of Excellence Publications, 2010, 47 à la p 47.

146 Yoshio Katayama, « Redefinition of the Concept of Low-Intensity Conflict » (2002) 3 National Institute for Defense Studies Security Reports 56 à la p 56.

économiques, d'information et militaires » [notre traduction][147]. Pour l'instant, la plupart des cyberattaques ont résulté en des dommages peu apparents. C'est cette « basse intensité inhérente aux cyberattaques »[148] qui explique la réticence des États à les qualifier de « faits de guerre »[149] lorsqu'elles surviennent. Avec leur faible coût de mise en œuvre, les cyberattaques étatiques viennent ainsi bouleverser les modes traditionnels de conflits et remettre en question l'actuel cadre normatif du *jus ad bellum*.

147 *Ibid*.

148 Louis-Sidney, *supra* note 115 à la p 77.

149 *Ibid* citant France, Ministère de la défense, *Un mutant juridique : l'agression internationale*, n° 7 Institut Recherche Stratégique École Militaire, 2011 à la p 67 (par Jean-Paul Pancracio et Emmanuel-Marie Peton).