La gendarmerie nationale, garante du continuum de sécurité face à la désinformation

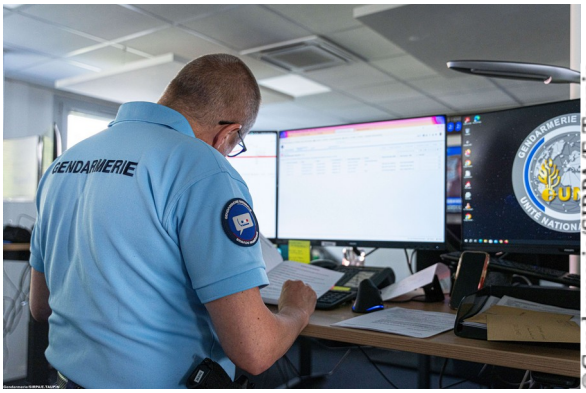
Cyprien Ronze-Spilliaert

LES NOTES DU CRGN

Centre de Recherche de la Gendarmerie Nationale

Numéro 107 – Octobre 2024

EV2 (RO) Cyprien RONZE-SPILLIAERT



©Gendarmerie/SIRPA/E.Taupin

Priorité stratégique de la prospective

Gendarmerie et territoires

Le CRGN certifie que ce document a été rédigé par un humain

LA GENDARMERIE NATIONALE, GARANTE DU *CONTINUUM* DE SÉCURITÉ FACE À LA DÉSINFORMATION

En juillet dernier, le Royaume-Uni a été frappé par une vague de violentes émeutes ciblant les migrants et les lieux de culte musulmans. Un drame et de fausses informations sont à l'origine de ces troubles à l'ordre public. Après qu'un jeune Britannique de 17 ans a assassiné trois fillettes à Southport, le 29 juillet 2024, de nombreux comptes d'ultra-droite et de mouvances néo-fascistes ont faussement indiqué que l'auteur de ces crimes était un immigré rwandais musulman et demandeur d'asile. Ces faits illustrent le rôle croissant de la désinformation dans l'insécurité et les troubles à l'ordre public. La désinformation consiste à diffuser un contenu d'informations « *faux ou inexact, créé avec l'intention délibérée d'induire les gens en erreur* », et « *susceptible de troubler l'ordre public* »[1].

Lorsque la désinformation est mise en œuvre par une puissance étrangère dans le but de « *provoquer l'impuissance ou l'affaiblissement de l'adversaire par le brouillage de son information et la désorientation de ses capacités de décision* »[2], il s'agit d'une ingérence informationnelle. Les avancées technologiques ont décuplé les possibilités de déstabilisation des sociétés par le biais de la désinformation avec la possibilité :

– de diffuser massivement des contenus faussés sur les réseaux sociaux par le biais d'usines à troll ou de bots ;

– de personnaliser ces contenus grâce à la marchandisation des données personnelles[3].

Les ingérences informationnelles cherchent à fracturer les sociétés, c'est-à-dire à accentuer les divisions entre les groupes sociaux, dans le but de favoriser les troubles à l'ordre public. Giuliano da Empoli, dans son ouvrage *Le Mage du Kremlin* (2022), a brillamment décrit cette « *stratégie du fil de fer* », désignant les ingérences informationnelles qui visent à radicaliser l'opinion publique en faveur des mouvances extrêmes[4]. *In fine*, les ingérences conduisent à l'affaiblissement du pays, de son économie, de ses forces morales[5] et, par conséquent, de sa capacité à se défendre. Dans le cadre d'un conflit armé de haute intensité, la désinformation peut ainsi constituer une technique de guerre psychologique visant « *à supprimer chez l'adversaire la volonté de combattre* »[6].

La lutte contre la désinformation et les ingérences informationnelles constitue donc autant un enjeu de défense nationale que de sécurité intérieure, vis-à-vis duquel la Gendarmerie nationale, en tant que force de sécurité intérieure (FSI) à statut militaire, joue un rôle singulier. En effet, la Gendarmerie est à même :

1 *Les Lumières à l'ère numérique.* Rapport de la commission présidée par Gérald BRONNER, 11 janvier 2022.
2 GÉRÉ, François. *Dictionnaire de la désinformation.* Armand Colin, 2011, 352 p.
3 Voir : MARTIN, Pascal. Les manipulations de l'information exploitent-elles des stratégies marketing ? [en ligne]. *Les Notes du CREOGN*, n° 100, mai 2024. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-crgn/note-n-100-manipulations-de-l-information-strategies-de-marketing
4 « *Nous tordons le fil de fer d'un côté, et nous le tordons de l'autre. Jusqu'à ce qu'il casse.* »
5 Le général Thierry Burkhard, chef d'état-major des armées, définit les forces morales comme « *la solidité de la cohésion nationale qui est notre centre de gravité, c'est-à-dire une source de puissance* ». Voir : Les forces morales, « l'énergie qui met en mouvement les individus, le ciment qui soude le collectif » [en ligne]. *Site de l'Académie de défense militaire*, 1er décembre 2023. Disponible sur : https://www.defense.gouv.fr/academ/actualites/forces-morales-lenergie-qui-met-mouvement-individus-ciment-qui-soude-collectif
6 Rapport d'information de l'Assemblée nationale du 17 février 2022 sur la préparation à la guerre de haute intensité.

– d'assurer le *continuum* de sécurité dans la sphère informationnelle, c'est-à-dire de protéger la population face à l'ensemble du spectre de la menace, allant de la désinformation anecdotique à la guerre psychologique de haute intensité ;
– de lutter contre les opérations d'ingérence informationnelle *intégrales* (opérations menées par des moyens militaires combinant actions de déstabilisation dans les champs physique – sabotages, saccages…– et numérique) ;
– de lutter contre les rétroactions à caractère informationnel sur le territoire national dans le contexte d'un conflit de haute intensité.

I) Ces dernières années, la France a renforcé son dispositif de lutte contre les attaques informationnelles

Sur le territoire national, la détection des ingérences informationnelles est pilotée par le Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), créé en 2021 et rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN). Fin 2023, Viginum a dévoilé l'existence d'un vaste réseau de près de 200 sites Internet pro-russes, baptisé Portal Kombat, diffusant des contenus faussés de propagande pro-russe. L'objectif de cette campagne de désinformation était de « *couvrir le conflit russo-ukrainien en présentant positivement "l'opération militaire spéciale" et en dénigrant l'Ukraine et ses dirigeants* »[7].

La Gendarmerie nationale, avec son Unité nationale cyber (UNC), est impliquée dans la lutte contre les ingérences. En effet, les entités étatiques hostiles menant des ingérences constituent l'un des quatre acteurs[8] de la menace cyber, contre laquelle lutte l'UNC[9]. Par ailleurs, les forces de l'ordre sont impliquées, au titre de la police administrative et de la police judiciaire, dans la lutte contre les ingérences informationnelles dans le champ physique, qui se sont multipliées ces derniers mois en France. Par exemple, les affaires des cercueils placés au pied de la tour Eiffel (juin 2024), des mains rouges sur le mur de la Shoah (mai 2024) et des étoiles de David taguées sur des murs parisiens (octobre 2023) ont toutes été orchestrées par des réseaux russes dans le but de déstabiliser la société française et ont fait l'objet d'enquêtes judiciaires.

Le ministère de l'Europe et des Affaires étrangères (MEAE) a mis en place, fin 2023, une sous-direction de la Veille et de la Stratégie, qui a pour mission de détecter les attaques informationnelles ciblant les intérêts français à l'étranger et de coordonner la riposte. Ainsi, en juin 2024, le MEAE a détecté une vidéo de désinformation diffusée sur X par l'ambassade de Russie à Pretoria, montrant un faux militaire français capturé en Ukraine par des soldats russes et s'exprimant avec un fort accent slave. L'objectif était de faire croire que la France avait envoyé des troupes se battre en Ukraine. Le ministère a rapidement réagi par le biais du compte de l'ambassade de France à Pretoria en suggérant, avec humour, d'inscrire l'acteur russe à des cours de français à l'Alliance française.

Sur le plan militaire, le ministère des Armées met en œuvre une défense informationnelle pour détecter et répondre aux attaques visant à porter atteinte à la réputation des forces armées. Ces dernières ont fortement augmenté depuis les années 2010 et le déploiement, en Afrique, du groupe Wagner, connu pour son activisme dans les opérations de guerre psychologique. L'affaire du charnier de Gossi, au Mali, illustre l'agressivité des attaques informationnelles ciblant l'armée française : en avril 2022, des mercenaires russes ont créé un faux charnier dans lequel ils ont enseveli des corps, puis ont diffusé sur les réseaux sociaux des photographies en accusant l'armée française d'un massacre. Des drones français ayant surpris la manœuvre ont permis de révéler le subterfuge. En janvier 2023, le groupe Wagner a publié un clip de propagande anti-France, représentant les soldats français sous la forme de zombies cadavériques cherchant à envahir l'Afrique.

Pour lutter contre ces opérations de guerre informationnelle, le ministère des Armées a créé en 2012 le Centre interarmées des actions dans l'environnement (CIAE), dont la mission consiste « *à mieux faire comprendre et accepter l'action de nos forces en opération auprès des acteurs locaux et ainsi gagner leur confiance* » (ministère des Armées). En outre, pour répondre aux attaques informationnelles dans le champ numérique, le ministère s'est doté en 2021 d'une doctrine de lutte informatique d'influence (L2I), qui « *désigne les opérations militaires conduites dans la couche informationnelle du cyberespace pour y détecter, caractériser et contrer les attaques* ». Les opérations de L2I relèvent du COMCYBER de l'état-major des armées.

II) La désinformation et les ingérences informationnelles constituent une menace importante pour la sécurité intérieure

La désinformation s'est accélérée ces dernières années avec, d'une part, l'arrivée sur le marché de réseaux sociaux permettant une instantanéité toujours plus grande et, d'autre part, la crise sanitaire, propice à la diffusion de *fake news* et

7 Viginum, février 2024, *Portal Kombat, Un réseau structuré et coordonné de propagande prorusse*.
8 Les trois autres types d'acteurs sont : « *les opportunistes en quête de notoriété, les groupes criminels organisés en quête d'enrichissement et les hacktivistes (hackers avec des revendications radicales)* ».
9 Entretien avec le colonel Hervé PÉTRY, commandant l'UNC. L'unité nationale cyber, des enquêteurs numériques au plus près de citoyens [en ligne]. *Inf'ONISTS,* n° 7, 3e trimestre 2024, p. 4-5. Disponible sur : https://www.calameo.com/read/0027192926788eedffd70

d'idées complotistes[10] (à l'instar du film *Hold Up*, en 2020). Les ingérences informationnelles se sont également accrues dans le contexte de la désinhibition de puissances étrangères hostiles, du retour de la guerre de haute intensité en Ukraine et de l'hybridation de la compétition inter-étatique.

Par conséquent, la désinformation constitue désormais un enjeu prioritaire de sécurité intérieure, notamment en raison des troubles à l'ordre public qu'elle est susceptible de provoquer ou d'attiser. Ainsi, l'assaut du Capitole aux États-Unis, en janvier 2021, a été rendu possible par la diffusion massive de *fake news* émanant notamment de groupe conspirationnistes (comme QAnon). En France, les émeutes urbaines de juin 2023 « *ont également été l'œuvre d'une instrumentalisation des réseaux sociaux* », comportant « *la diffusion de fausses informations* »[11]. Ainsi, des *fake news* massivement diffusées sur les réseaux sociaux ont attisé la violence des émeutiers, comme par exemple un faux communiqué du ministère de l'Intérieur indiquant qu'Internet serait coupé à certaines heures dans les quartiers sensibles. Plus récemment, les émeutes en Nouvelle-Calédonie ont été attisées par des comptes azéris diffusant sur les réseaux des montages photos ou vidéos « *accusant la police française de tuer des manifestants indépendantistes* ».[12]

III) La Gendarmerie dispose des moyens d'assurer le *continuum* de sécurité dans le champ informationnel

Par sa polyvalence, son identité militaire et son expertise dans le domaine cyber, la Gendarmerie est en mesure d'assurer le *continuum* de sécurité dans le champ informationnel, c'est-à-dire de lutter contre l'ensemble du spectre de la menace.

La lutte contre la désinformation, aussi bien dans l'espace physique que numérique, nécessite une approche pluridisciplinaire, correspondant aux différents savoir-faire de la Gendarmerie :

– renseignement criminel : les puissances hostiles utilisent souvent des groupes criminels organisés (GCO) comme *proxies* pour réaliser des manœuvres de déstabilisation, de désinformation ou de sabotage sur le territoire national (à l'instar de sabotages sur des voies ferrées en Allemagne et d'incendies criminels en Pologne commandités par des réseaux russes). Les *proxies* permettent de masquer l'implication de la puissance commanditaire[13]. La Gendarmerie dispose, avec son Service central de renseignement criminel (SCRC), son Office central de lutte contre la délinquance itinérante (OCLDI) et ses groupes d'observation et de surveillance (GOS), de moyens importants de lutte contre le crime organisé et, par conséquent, les *proxies* de puissances étrangères :

– police judiciaire : avec ses sections de recherche et son Institut de recherche criminelle (IRCGN), la Gendarmerie est en mesure de mener à bien les enquêtes judiciaires pour rassembler les preuves permettant d'identifier les auteurs d'actions de manipulation de l'information ;

– lutte contre les criminalités numériques : les manipulations de l'information sont diffusées massivement dans le cyberespace. Avec son Unité nationale cyber (et plus précisément son Centre de lutte contre les criminalités numériques – C3N) et ses 10 000 gendarmes formés aux enquêtes dans le cyberespace, la Gendarmerie dispose de l'expertise nécessaire à la détection rapide de désinformations et ingérences informationnelles numériques, et à la réalisation des enquêtes judiciaires afférentes[14] ;

– sécurité publique : le maillage territorial de la Gendarmerie lui permet d'intervenir sur la quasi-totalité du territoire pour prévenir et lutter contre les actions de sabotage ou de saccage concourant à des objectifs de manipulation de l'opinion publique[15].

En outre, la Gendarmerie peut être engagée en amont et en aval de la menace informationnelle :

– *en amont*, avec des actions de sensibilisation face aux risques d'ingérences étrangères et de diffusion de fausses informations. Avec ses brigades de gendarmerie départementale, l'Institution dispose d'un maillage territorial dense, en particulier dans les zones ciblées par les ingérences, comme les départements et régions d'outre-mer et les collectivités

10 Dans son article « *Fake news* et théories du complot en période(s) pandémique(s) », de février 2020 (revue *Quaderni*), Julien Giry explique comment la crise sanitaire a été une « *fenêtre d'opportunité pour les discours conspirationnistes et les* fake news ».

11 HASNAOUI, Donya. Les jeunes et la guérilla informationnelle [en ligne]. *Les Notes du CREOGN*, note n° 99, avril 2024. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/note-n-99

12 Fiche technique de VIGINUM, SGDSN, 17 mai 2024.

13 Commission de la défense nationale et des forces armées, 17/02/2022, *Rapport d'information sur la préparation à la haute intensité (Rapport d'information n° 5054)*, Assemblée nationale.

14 LESUEUR, François-Xavier. Communication et influence à l'ère numérique : quels enjeux pour la Gendarmerie nationale ? *Revue de la défense nationale*, août 2022: « *Lorsqu'un contenu illicite est détecté, les cybergendarmes* (…) *s'engagent, sous le contrôle des magistrats, dans des investigations judiciaires qui permettent* (…) *de poursuivre les émetteurs des contenus mais aussi les relayeurs et les plateformes*. »

15 Par exemple, un groupe criminel organisé pourrait saboter une infrastructure critique puis mener en parallèle des actions informationnelles dans l'espace numérique pour en imputer la responsabilité à un groupe activiste ou à une frange de la population, afin d'accroître les tensions et les divisions au sein de la population. Ainsi, l'opération dans le champ physique des mains rouges sur le mur de la Shoah avait fait l'objet d'une amplification numérique sur le réseau X.

d'outre-mer (DROM-COM). L'action de sensibilisation de la Gendarmerie aux risques d'influences étrangères a ainsi été saluée par la sénatrice Nathalie Goulet[16] ;

– *en aval*, avec le maintien et le rétablissement de l'ordre à la suite de troubles consécutifs à des manipulations de l'information. Les unités de gendarmerie mobile sont en mesure de prévenir de tels troubles grâce aux renseignements précoces fournis par les unités de renseignement criminel et cyber.

En somme, l'ensemble des métiers de la Gendarmerie forme une chaîne cohérente permettant d'appréhender les phénomènes de désinformation avec une approche holistique.

Enfin, par son statut militaire, la gendarmerie est en mesure de faire face à toutes les intensités de la menace informationnelle[17]. Elle peut naturellement intervenir dans le cadre d'actions de désinformation anecdotiques. En effet, la désinformation est une infraction pénale punie par la loi[18]. Elle peut également être engagée face à des dispositifs de véritable guerre psychologique, combinant par exemple sabotages d'infrastructures critiques par des forces spéciales étrangères[19] et opérations d'ampleur de désinformation sur les réseaux sociaux. Il s'agit alors d'ingérences informationnelles pouvant être qualifiées *d'intégrales,* car elles utilisent des moyens militaires, investissent les champs aussi bien physique que numérique et combinent l'ensemble des techniques destinées à manipuler l'information (manœuvres cyber, sabotages, saccages, amplification sur les réseaux sociaux, etc.).

Enfin, en cas de participation de la France à un conflit de haute intensité, la Gendarmerie serait en première ligne face aux potentielles rétroactions de l'adversaire[20], c'est-à-dire des attaques sur le territoire national sous le seuil de l'affrontement, dans l'objectif d'affaiblir et de déstabiliser. Les manœuvres de désinformation et de sabotage[21] figurent au premier rang des rétroactions envisagées. Elles auraient pour objectif :

– d'affaiblir les forces morales et donc la volonté du pays à poursuivre le combat ;

– de provoquer de graves troubles à l'ordre public, en renforçant les groupes contestataires et les groupuscules violents par une radicalisation de l'opinion publique.

La gendarmerie, en tant que force de sécurité intérieure sous statut militaire, est la plus à même de lutter contre les rétroactions informationnelles, éventuellement accompagnées de sabotages. En effet, les gendarmes, formés au combat militaire, pourraient neutraliser des groupes ennemis[22] – jusqu'à environ dix combattants – infiltrés afin de mener une guerre psychologique sur le territoire national. L'action des gendarmes serait facilitée par l'utilisation des capacités de renseignement de la gendarmerie dans les champs physique et informationnel. Enfin, la militarité de la Gendarmerie la rend interopérable avec les armées dans la lutte contre les rétroactions.

Le caractère militaire de la Gendarmerie nationale offre un véritable atout stratégique pour lutter contre la désinformation et les ingérences informationnelles étrangères. Par sa polyvalence, son interopérabilité avec la police nationale et les forces armées ainsi que par sa capacité d'adaptation et son maillage territorial, la Gendarmerie est un acteur incontournable de la défense informationnelle du territoire. Il serait pertinent d'aller plus loin avec l'élaboration d'une doctrine de lutte informatique d'influence propre à la Gendarmerie, à l'instar du ministère des Armées.

Diplômé de l'École normale supérieure Paris-Saclay et du master Projet-Innovation-Conception de l'École polytechnique, ***Cyprien Ronze-Spilliaert*** *est un ancien officier de la réserve opérationnelle spécialiste de la Gendarmerie nationale, où il occupait un poste d'analyste en renseignement stratégique au Service central de renseignement criminel. Il est désormais officier de la réserve opérationnelle de la Marine nationale, affecté à l'état-major des armées. Dans le civil, il est économiste au sein d'une direction d'administration centrale d'un ministère.*

16 À l'occasion de l'audition du ministre des Armées, le 25 juin 2024, Madame Goulet rendait ainsi hommage à la Gendarmerie : « *Les gendarmes accomplissent un énorme travail auprès de populations ciblées pour les prévenir. Ici même, des actions de sensibilisation aux influences étrangères ont été menées*. » Disponible sur : https://www.senat.fr/compte-rendu-commissions/20240624/ce_influences.html

17 Dans son article de juillet 2023, « Lutter contre les rétroactions sur le territoire national, quel rôle pour la Gendarmerie nationale ? », publié dans la *Revue de la défense nationale,* le colonel Tugdual Vieillard-Baron souligne que la polyvalence de la Gendarmerie la rend apte à assurer le *continuum* de sécurité face à des actions de déstabilisation – notamment informationnelle – sur le territoire national : « *Grâce au statut militaire des gendarmes aux capacités dont elle dispose, la Gendarmerie est en mesure d'assurer le* continuum *de sécurité entre défense civile et défense militaire, et de coopérer avec les armées dans cette lutte.* »

18 Article 27 de la loi du 29 juillet 1881.

19 Commission de la défense nationale et des forces armées, *Rapport d'information sur la préparation à la haute intensité (Rapport n° 5054)*, Assemblée nationale, 17 février 2022, citant la DRSD : en cas de conflit de haute intensité, « *l'adversaire aurait certainement recours à « des actions de déstabilisation sur le territoire national, en s'appuyant sur des proxies et/ou par l'infiltration de forces spéciales* ».

20 Commission de la défense nationale et des forces armées, 12/10/2022, « Audition du général d'armée Pierre Schill sur le PMF 2022 », Assemblée nationale.

21 VIEILLARD-BARON, Tugdual. Lutter contre les rétroactions sur le territoire national, quel rôle pour la Gendarmerie nationale ? [en ligne] *Revue de la défense nationale*, juillet 2023 : « *L'ennemi cherchera aussi à mener des actions plus discrètes, accidentelles, de sabotage* (…) e*t, en manipulant des groupes contestataires ou communautaristes, à provoquer des troubles sociétaux graves (manifestations, émeutes, zones de non-droit). Il mènera également des* (…) *actions d'influence pour faire douter du bien-fondé du combat.* » Disponible sur : https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=602&cidcahier=1320

22 Réponse du ministère de la Défense à la question écrite n° 14722 de M. Hubert Haenel, mai 1999.

ISSN : 2428-7733