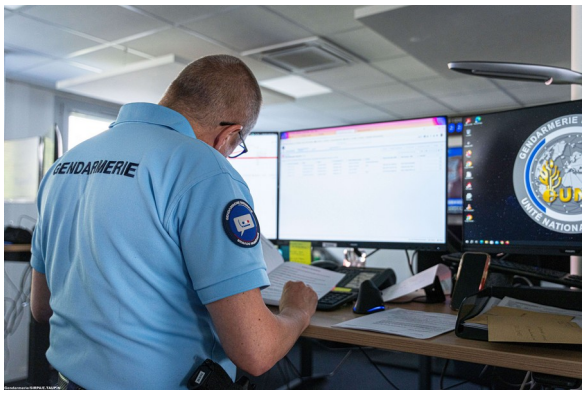
The CRGN Research Notes

French Gendarmerie Research Center

Issue 107 – October 2024

EV2 (RO) Cyprien RONZE-SPILLIAERT



©Gendarmerie/SIRPA/E.Taupin

Priorité stratégique de la prospective

Gendarmerie et territoires

CRGN certifies that this document was written by a human intelligence

THE GENDARMERIE, GUARANTOR OF THE SECURITY *CONTINUUM* IN THE FACE OF DISINFORMATION

In July last year, the United Kingdom was struck by a wave of violent riots targeting migrants and Muslim places of worship. A tragedy and false information were at the origin of these public order disturbances. After a 17-year-old British youth murdered three young girls in Southport on July 29, 2024, numerous far-right and neo-fascist accounts falsely claimed that the perpetrator of these crimes was a Rwandan Muslim immigrant and asylum seeker. These events illustrate the growing role of disinformation in insecurity and public disorder. Disinformation consists of spreading information that is "*false or inaccurate, created with the deliberate intention to mislead people*", and "*likely to disturb public order*"[1].

When disinformation is carried out by a foreign power with the goal of "*causing impotence or weakening the adversary by disrupting their information and disorienting their decision-making capabilities*"[2], it constitutes informational interference. Technological advancements have greatly enhanced the ability to destabilize societies through disinformation, including the possibility:

– to massively disseminate distorted content on social media via troll farms or bots;

– to personalize this content thanks to the commercialization of personal data[3].

Informational interference seeks to fracture societies—that is, to exacerbate divisions between social groups—in order to promote public disorder. Giuliano da Empoli, in his book *Le Mage du Kremlin* (2022), brilliantly described this "*barbed wire strategy*", referring to informational interference that aims to radicalize public opinion in favor of extremist movements[4]. Ultimately, such interference leads to the weakening of the country, its economy, its moral strength[5], and consequently, its ability to defend itself. In the context of high-intensity armed conflict, disinformation may thus constitute a technique of psychological warfare aimed at "*eliminating the adversary's will to fight*"[6].The fight against disinformation and informational interference is therefore both a matter of national defense and internal security, in which the National Gendarmerie, as an internal security force (ISF) with military status, plays a unique role. Indeed, the Gendarmerie is capable of:

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 See : MARTIN, Pascal. Les manipulations de l'information exploitent-elles des stratégies marketing ? [online]. *Les Notes du CREOGN*, n° 100, mai 2024. Avalaible at : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-crgn/note-n-100-manipulations-de-l-information-strategies-de-marketing
4 "*We twist the wire on one side, and we twist it on the other. Until it breaks*."
5 General Thierry Burkhard, Chief of the Defence Staff, defines moral forces as "*the solidity of national cohesion, which is our centre of gravity, in other words a source of power*". See : Les forces morales, « l'énergie qui met en mouvement les individus, le ciment qui soude le collectif » [online]. *Site de l'Académie de défense militaire*, 1er décembre 2023. Avalaible at : https://www.defense.gouv.fr/academ/actualites/forces-morales-lenergie-qui-met-mouvement-individus-ciment-qui-soude-collectif
6 National Assembly information report of 17 February 2022 on preparedness for high-intensity warfare.

– ensuring the security continuum in the information sphere, i.e., protecting the population from the entire spectrum of threats, ranging from anecdotal disinformation to high-intensity psychological warfare;
– fighting against comprehensive informational interference operations (operations conducted by military means combining destabilization actions in physical fields—sabotage, vandalism—and digital fields);
– combating informational feedback effects on national territory in the context of high-intensity conflict.

I) In recent years, France has strengthened its system for combating informational attacks

On national territory, the detection of informational interference is led by the Service for Vigilance and Protection against Foreign Digital Interference (Viginum), created in 2021 and linked to the General Secretariat for Defense and National Security (SGDSN). At the end of 2023, Viginum revealed the existence of a vast network of nearly 200 pro-Russian websites, named *Portal Kombat*, disseminating falsified pro-Russian propaganda content. The objective of this disinformation campaign was to "*cover the Russian-Ukrainian conflict by portraying the 'special military operation' positively and denigrating Ukraine and its leaders*"[7].
The National Gendarmerie, through its National Cyber Unit (UNC), is involved in the fight against interference. Indeed, hostile state entities conducting interference operations are one of the four types of cyber threats[8] that the UNC combats[9]. Moreover, law enforcement is involved, under administrative and judicial police powers, in the fight against informational interference in the physical realm, which has increased in recent months in France. For example, the cases of coffins placed at the foot of the Eiffel Tower (June 2024), red handprints on the Shoah memorial wall (May 2024), and Stars of David sprayed on Parisian walls (October 2023) were all orchestrated by Russian networks with the aim of destabilizing French society and led to judicial investigations.
The Ministry of Europe and Foreign Affairs (MEAE) set up, at the end of 2023, a Sub-Directorate for Monitoring and Strategy, whose mission is to detect informational attacks targeting French interests abroad and to coordinate the response. Thus, in June 2024, the MEAE detected a disinformation video broadcast on X by the Russian Embassy in Pretoria, showing a fake French soldier captured in Ukraine by Russian soldiers, speaking with a strong Slavic accent. The aim was to make people believe that France had sent troops to fight in Ukraine. The ministry quickly responded through the French Embassy's X account in Pretoria, humorously suggesting that the Russian actor enroll in French classes at the *Alliance Française*.
On the military level, the Ministry of the Armed Forces is implementing informational defense to detect and respond to attacks aimed at harming the reputation of the armed forces. These attacks have increased significantly since the 2010s and the deployment in Africa of the Wagner Group, known for its activism in psychological warfare operations. The *Gossi mass grave case*, in Mali, illustrates the aggressiveness of informational attacks targeting the French army: in April 2022, Russian mercenaries created a fake mass grave where they buried bodies and then posted photos on social media accusing the French army of a massacre. French drones, which captured the maneuver, exposed the deception. In January 2023, the Wagner Group released an anti-France propaganda video portraying French soldiers as zombie-like corpses trying to invade Africa.
To counter these information warfare operations, the Ministry of the Armed Forces created, in 2012, the Joint Centre for Actions in the Environment (CIAE), whose mission is "*to better explain and promote the actions of our forces during operations to local actors and thus earn their trust*" (Ministry of the Armed Forces). In addition, to respond to digital informational attacks, the ministry adopted, in 2021, an influence cyber warfare doctrine (L2I), which "*refers to military operations conducted within the information layer of cyberspace to detect, characterize, and counter attacks*". L2I operations fall under the COMCYBER of the Armed Forces General Staff.

II) Disinformation and informational interference constitute a major threat to internal security

Disinformation has accelerated in recent years due, on the one hand, to the arrival on the market of social networks enabling ever-greater immediacy, and on the other hand, to the health crisis, which provided fertile ground for the dissemination of fake news and conspiracy theories[10] (such as the film *Hold Up* in 2020). Informational

7 Viginum, février 2024, Portal Kombat, Un réseau structuré et coordonné de propagande prorusse.
8 The other three types of actor are: "*opportunists seeking notoriety, organised crime groups seeking enrichment and hacktivists (hackers with radical demands)*".
9 Entretien avec le colonel Hervé PÉTRY, commandant l'UNC. L'unité nationale cyber, des enquêteurs numériques au plus près de citoyens [online]. *Inf' ONISTS*, n° 7, 3e trimestre 2024, p. 4-5. Available at : https://www.calameo.com/read/0027192926788eedffd70

interference has also increased in the context of emboldened hostile foreign powers, the return of high-intensity warfare in Ukraine, and the hybridization of interstate competition.

As a result, disinformation now represents a priority issue for internal security, particularly due to the public order disturbances it can provoke or exacerbate. For instance, the assault on the U.S. Capitol in January 2021 was made possible by the massive spread of fake news, especially from conspiracy groups (like QAnon). In France, the urban riots of June 2023 "*were also driven by the exploitation of social networks*", which involved the "*dissemination of false information*"[11]. For example, fake news massively circulated on social media fueled the rioters' anger, such as a fake press release from the Ministry of the Interior stating that the Internet would be shut down at specific hours in certain sensitive neighborhoods. More recently, riots in New Caledonia were stirred up by Azerbaijani accounts spreading fake photo and video montages on social media, "accusing French police of killing pro-independence protesters"[12].

III) The Gendarmerie has the means to ensure the security *continuum* in the informational domain

Thanks to its versatility, military identity, and expertise in the cyber domain, the Gendarmerie is capable of ensuring the security *continuum* in the informational sphere, that is, to combat the full spectrum of threats.

The fight against disinformation—whether in the physical or digital space—requires a multidisciplinary approach, aligned with the Gendarmerie's various areas of expertise:
– Criminal intelligence: Hostile powers often use organized criminal groups (OCGs) as proxies to carry out destabilization, disinformation, or sabotage operations on national territory (such as sabotaged railways in Germany and arson attacks in Poland orchestrated by Russian networks). These proxies make it possible to conceal the involvement of the initiating power[13]. The Gendarmerie possesses substantial resources to combat organized crime—and therefore these proxies—through its Central Criminal Intelligence Service (SCRC), Central Office for Combating Itinerant Crime (OCLDI), and Observation and Surveillance Groups (GOS).
– Judicial police: Through its investigative sections and Criminal Research Institute (IRCGN), the Gendarmerie can conduct judicial investigations to gather evidence identifying the perpetrators of information manipulation.
– Combating digital crime: Information manipulation is widely spread through cyberspace. With its National Cyber Unit (and more precisely its Center for Combating Digital Crime – C3N) and its 10,000 gendarmes trained in cyber investigations, the Gendarmerie has the expertise necessary for the rapid detection of disinformation and digital informational interference, as well as for conducting the related judicial investigations[14].
– Public security: The Gendarmerie's territorial presence allows it to intervene across nearly the entire national territory to prevent and combat sabotage or vandalism actions intended to manipulate public opinion[15].
Moreover, the Gendarmerie can be engaged both upstream and downstream of the informational threat:
– Upstream, through awareness campaigns addressing the risks of foreign interference and fake news dissemination. With its departmental brigades, the Institution benefits from a dense territorial network, particularly in zones targeted by interference, such as overseas departments and regions and overseas collectivities (DROM-COM). The Gendarmerie's awareness efforts on foreign influence risks have been commended by Senator Nathalie Goulet[16].

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 [online]. *Les Notes du CREOGN*, note n° 99, avril 2024. Available at : 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 For instance, an organised criminal group could sabotage a critical infrastructure and then at the same time carry out informational actions in digital space to blame an activist group or a section of the population, in order to increase tensions and divisions within the population. For example, the operation in the physical field of the red hands on the Shoah wall was digitally amplified on Network X.

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*. ». Available at: https://www.senat.fr/compte-rendu-commissions/20240624/ce_influences.html

– Downstream, by maintaining and restoring order following public disturbances caused by information manipulation. Mobile Gendarmerie units are capable of preventing such disturbances thanks to early intelligence gathered by criminal and cyber intelligence units.
In summary, the Gendarmerie's full range of specialties forms a coherent chain, allowing for a holistic approach to disinformation.
Finally, due to its military status, the Gendarmerie is able to respond to all levels of informational threat[17]. It can naturally act in the face of anecdotal disinformation. Indeed, disinformation is a criminal offense punishable by law[18]. It can also respond to true psychological warfare devices, combining, for example, critical infrastructure sabotage by foreign special forces[19] and large-scale disinformation operations on social media. These are comprehensive informational interference operations, as they use military means, span both physical and digital domains, and combine all known disinformation techniques (cyber maneuvers, sabotage, vandalism, social media amplification, etc.).
Finally, in the event of France's participation in a high-intensity conflict, the Gendarmerie would be on the front line in facing potential adversarial feedback actions[20] —that is, attacks on national territory below the threshold of open conflict, aimed at weakening and destabilizing the country. Disinformation and sabotage maneuvers[21] would be at the forefront of such feedback actions. Their objectives would be:
– to weaken the moral forces, and therefore the country's will to continue fighting;
– to provoke serious disturbances to public order, by reinforcing protest movements and violent fringe groups through the radicalization of public opinion.
The Gendarmerie, as an internal security force with military status, is best equipped to counter informational feedback actions, which may also involve acts of sabotage. Trained in military combat, gendarmes could neutralize enemy groups[22]—up to around ten fighters—who have infiltrated national territory to conduct psychological warfare. Their actions would be supported by the Gendarmerie's intelligence capabilities across both the physical and informational domains. Finally, the military nature of the Gendarmerie makes it interoperable with the armed forces in the fight against these feedback actions.

The military status of the National Gendarmerie thus represents a genuine strategic asset in the fight against disinformation and foreign informational interference. Thanks to its versatility, interoperability with the National Police and Armed Forces, adaptive capabilities, and territorial network, the Gendarmerie is an essential actor in the information defense of the country. It would be pertinent to go further by developing a specific doctrine of influence cyber warfare for the Gendarmerie, similar to that adopted by the Ministry of the Armed Forces.

Having graduated from the École normale supérieure Paris-Saclay and the Project-Innovation-Design master's program of École Polytechnique, ***Cyprien Ronze-Spilliaert*** *is a former officer of the operational reserve specializing in the National Gendarmerie, where he served as a strategic intelligence analyst at the Central Criminal Intelligence Service. He is currently a naval reserve officer assigned to the General Staff of the Armed Forces. In civilian life, he is an economist in a central administration department of a ministry.*

Translated by Aude Grégory, Reserve assistant gendarme

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 ? [online] *Revue de la défense nationale*, juillet 2023 : « *L'ennemi cherchera aussi à mener des actions plus discrètes, accidentelles, de sabotage (…) et, 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*. » Available at : 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.