The CREOGN Research Notes

French Gendarmerie Officers Academy Research Centre

Issue 100 – May 2024

Captain Pascal MARTIN (Dr)

CREOGN
CENTRE DE RECHERCHE

©Image générée par l'IA de Microsoft

Strategic priority of foresight

The Future of Digital Territories

CREOGN certifies that this document was written by a human

DOES THE MANIPULATION OF INFORMATION MAKE USE OF MARKETING STRATEGIES?

In his work *The Art of War*, Sun Tzu emphasizes the psychological dimension of conflict, which allows one to secure the enemy's surrender while minimizing combat. Consequently, the use of information to undermine enemy morale is a central issue, for "*false, manipulated, or subverted information is a weapon.*"[1] In France, these risks had already been identified and addressed under Article 27 of the Law of July 29, 1881, on freedom of the press.[2]

The offensive potential of information can be applied more broadly to other fields and expanded through the new capabilities for disseminating information made possible by new information and communication technologies (NICTs). It is therefore no longer limited to armed conflict alone and can be incorporated into strategies of influence by manipulating public opinion for strategic purposes.

Furthermore, technological innovation makes it possible to reach a mass audience while also personalizing messages to "*an extreme degree.*"[3] This is made possible by the reach of social media, as well as the collection and analysis of data generated by internet users. Information is thus disseminated with greater granularity. However, while information is disseminated on the cognitive layer of cyberspace, it is also on this layer that it is exploited to carry out a large portion of manipulation operations.[4]

If their effectiveness relies on exploiting our physiological weaknesses, what synergies might exist with marketing strategies?[5]

I) Does misinformation fulfill a physiological need?

A term of Soviet origin (dezinformatsiya) coined in the 1920s[6] to denounce the information warfare operations of which the USSR was allegedly a victim[7], Disinformation "*is the first intelligent weapon that man has ever put into*

1 PARLY, Florence, ministre des Armées. In : MINISTÈRE DES ARMÉES. *Florence Parly présente la doctrine militaire de lutte informatique d'influence* [online]. Website of the Ministry of Armed Forces, October 21st 2021. Available via: https://archives.defense.gouv.fr/portail/actualites2/florence-parly-presente-la-doctrine-militaire-de-lutte-informatique-d-influence.html

2 Article 27 of the Law of July 29, 1881, on Freedom of the Press: "*The publication, dissemination, or reproduction, by any means whatsoever, of false news, fabricated documents, forged documents, or documents falsely attributed to third parties, when done in bad faith and resulting in a disturbance of the public peace, or likely to cause such a disturbance, shall be punishable […]. The same acts shall be punishable […], when the publication, dissemination, or reproduction, made in bad faith, is likely to undermine the discipline or morale of the armed forces or to hinder the nation's war effort.*"

3 REMANJON, Jérôme. Le cerveau humain sera-t-il l'ultime champ de bataille ? *Revue Défense Nationale*, tribune n° 1277, 2021, p. 3.

4 LACHAUD, Bastien, VALETTA-ARDISSON, Alexandra. *Rapport d'information sur la cyberdéfense,* 2018, p. 19.

5 Marketing involves analyzing consumer preferences and the strategies organizations can use to influence consumer behavior.

6 LECOMTE, Bernard. *KGB. La véritable histoire des services secrets soviétiques.* Paris : éditions Perrin, 2020, p. 51.

7 JEANGÈNE VILMER, Jean-Baptiste. La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande ? Comité d'études de la Défense nationale, *Revue Défense Nationale*, n° 801, 2017, p. 95.

practice."[8] This can be defined as "*an action that involves getting a recipient—whom one intends to deceive—to accept a certain description of reality that is favorable to the sender, by presenting it as reliable and verified information*"[9], it serves as a means of achieving policy objectives.[10] Iouri Andropov, leader of the KGB[11] from 1967 to 1982, believed that "*misinformation is like cocaine. If you use it once or twice, it's not likely to change your life. However, daily use will turn you into an addict—and thus, a completely different person.*"[12] Noting that this is an issue that warrants further investigation, the Canadian Security Intelligence Service (CSIS)[13] questions Andropov's statements: it can be assumed that he believed disinformation has a physiological aspect in that it captures attention and impairs the critical thinking abilities of those who consume it. In this context, "*it is as if the human brain contained a 'disinformation receptor' which, once stimulated, convinces it that it wants more."*[14] Thus, "*many people consume fake news like junk food: knowing it's bad for them but doing it anyway for the sheer pleasure of it.*"[15]

In 1999, Russian strategist Sergey Rastorguev outlined his views in a book published with the support of the FSB[16], how to manipulate the human mind and "*algorithmically model individual behavior.*"[17] The author believes that human beings, like computer systems, can have their thought processes disrupted by a "*virus*" known as a "*psychovirus.*"[18] The growing prevalence of digital technology would thus serve to amplify this presumed physiological aspect[19], because it exposes people to information overload and, as a result, to the risk of encountering manipulated information. This phenomenon is particularly pronounced among young adults: information consumption is increasingly taking place *through* digital services.[20] However, these companies employ behavioral psychology strategies to create user dependency[21]: For example, social media platforms use the proliferation of social interactions "*as a dopamine rush*" to create addiction.[22]

II) Marketing techniques used to further disinformation campaigns

A study funded by the North Atlantic Treaty Organization (NATO) in 2020 estimated that marketers have long understood that the brain is the seat of attention and decision-making and, as such, they seek to understand it, anticipate its choices, and influence it.[23] Nevertheless, the field of cognitive science is not of interest solely for its military applications[24]: Advertising and marketing "*are the two main vehicles for social propaganda.*"[25] As early as 1928, Edward Bernays, Sigmund Freud's nephew, outlined in his book *Propaganda* how to manipulate public opinion for economic or political ends. Marketing therefore aims to better understand the cognitive realm within a consumerist framework: scent marketing, store layout, the psychology of colors on packaging and in advertisements, the flow of traffic within stores, and so on.

Based on this premise, information manipulation and influence operations can rely on social engineering techniques[26] and marketing, to achieve more precise targeting and tailor messages to specific audiences. In this context, the digitization of lifestyles, production, and consumption enables a scale-up in the implementation of such operations and

8 BONNET, Yves. *Contre-espionnage. Mémoires d'un patron de la DST.* Paris : éditions Calmann-Lévy, 2000, p. 266.
9 BRETON, Philippe. *La parole manipulée*. Paris : La découverte, 2020, 198 p.
10 ARENDT, Hannah. *Du mensonge à la violence.* Paris : éditions Pocket, 2002, p. 8.
11 The Soviet Union's intelligence service from 1954 to 2011.
12 MIHKELSON, Marko. "Disinformation across ages: Russia's old but effective weapon of influence." *Euromaidan Press*, July 2017. Available via: https://icds.ee/en/disinformation-russias-old-but-effective-weapon-of-influence/
13 The Canadian Security Intelligence Service is Canada's primary intelligence agency.
14 CANADIAN SECURITY INTELLIGENCE SERVICE. *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui.* 2018, p. 27.
15 JEANGÈNE VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina. *Les manipulations de l'information – Un défi pour nos démocraties.* Report by the Center for Analysis, Forecasting, and Strategy (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research at the École Militaire (IRSEM) of the Ministry of the Armed Forces, Paris, 2018, p. 184.
16 The Federal Security Service of the Russian Federation, which has been Russia's intelligence agency responsible for internal security matters since 1991.
17 COLON, David. *La guerre de l'information. Les États à la conquête de nos esprits*. Paris: Tallandier, 2023, p. 271.
18 *Ibidem.*
19 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 14, p. 27.
20 WOITIER, Chloé. Les 15-24 ans, plus gros consommateurs d'internet en France. *Le Figaro*, February 16th 2023.
21 PATINO, Bruno. *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*. Paris : Le livre de poche, 2020, 168 p.
22 ABITEBOUL, Serge. CATTAN, Jean. *Nous sommes les réseaux sociaux.* Paris : éditions Odile Jacob, 2022, p. 65.
23 DU CLUZEL, François. *Cognitive Warfare.* Innovation Hub, 2020, p. 16.
24 « *L'action militaire repose sur les capacités techniques du ComCyber mais aussi sur des compétences culturelles, psychologiques ou de marketing numérique* ». In : BAROTTE, Nicolas. La France s'arme face à la guerre d'influence. *Le Figaro*, October 21st 2021, p. 7.
25 ABITEBOUL, Serge. CATTAN, Jean, *op. cit.* note 22, p. 139.
26 L'ingénierie sociale « […] *s'appuie sur la manipulation psychologique et exploite les erreurs ou les faiblesses humaines plutôt que les vulnérabilités techniques ou numériques des systèmes* […] » [online]. In : Qu'est-ce que l'ingénierie sociale ? *IBM*. Available via: https://www.ibm.com/fr-fr/topics/social-engineering

provides significant leverage in targeting. Thus, as early as 2019, the Ministry of the Armed Forces estimated that synergies could be found between digital influence, the fight against information manipulation operations, and marketing.[27]

While the manipulation of information (and more specifically disinformation) is characterized by and distinguished from marketing due to its objectives and the disregard for moral or ethical constraints, CSIS notes, however, that the methods used are similar to modern marketing practices.[28] In this context, we can cite the example of "neuromarketing," which refers to two closely related concepts: "*the study, through neuroscience, of how the human brain functions when exposed to stimuli, and the improvement of persuasion techniques.*"[29]

As such, the advertising industry is often viewed as a testing ground for disinformation, since the goal is to present facts or products in the best possible light for commercial purposes[30], after assessing the market's receptiveness to a product.[31] In addition, information manipulation techniques already employ a marketing method known as "A/B testing." This method allows for comparing the impact of two messages—referred to as "variables"—on a target audience: adjustments can then be made to refine the message based on which one is more viral, thereby increasing its effectiveness.[32]

Consequently, the tools developed in marketing would include two features that are useful for understanding the mechanisms of information manipulation[33]:

– on the one hand, by analyzing a target group's reaction to a specific campaign, these tools provide a better understanding of the impact—visual, emotional, rational, and intellectual—of a message on a given audience;

– on the other hand, by highlighting a message's weaknesses, as well as the reasons why a user might choose one message over another, they provide insights into how conventional media outlets deemed reliable can enhance their appeal and capture the attention of an audience that is currently beyond their reach.

III) The Blurring Lines Between Marketing and Intelligence

A growing trend has been observed in which intelligence agencies and online advertising services employ similar practices, particularly in the areas of geolocation and cyber-profiling. Furthermore, private intelligence firms and targeted marketing agencies are finding themselves faced with the need to collect ever-increasing amounts of digital data in order to improve targeting and operate as closely as possible to users.[34]

This trend is reflected in the hiring strategies of certain companies: Criteo, the French targeted advertising specialist, hired James Shinn in 2021, a former intelligence officer with the *Central Intelligence Agency* (CIA) and a technology expert.[35] As a result, firms that support election campaigns through aggressive online strategies are increasingly hiring former intelligence officers: CIY Global, a company chaired by the former head of the Mossad[36] Danny Yatom, also hired the former director of the BND[37], August Hanning. This company offers to identify and neutralize online troll groups, and to conduct its own offensive operations, including "*black ops*"[38], the details of which are to be determined with the client.[39]

According to industry publications, the General Directorate for External Security (DGSE) also appears to be interested in the manipulation of information through marketing practices. In 2017, the agency offered an internship titled "*How I Met Your Social Network Profile*" to recruit an expert in *big data*, artificial intelligence, and marketing.[40] The objective was to conduct applied research on the dissemination of information within social networks, the traceability of information, and the processes underlying the popularity and reach of messages and profiles, and thereby to identify the key factors influencing information dissemination and "*social media community management.*"[41] The use of

27 Department of the Armes Forces. *L'intelligence artificielle au service de la défense.* Report of the AI Task Force, 2019, p.17.

28 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 14, p. 27.

29 DELAYE, Claire. Le neuromarketing : l'attention, l'émotion et la mémoire [online]. In : *Site Spirit, source :* Digital effervescence*,* May 11th 2016. Available via: https://www.spiriit.com/blog/le-neuromarketing-lattention-lemotion-et-la-memoire/

30 GÉRÉ, François. *Dictionnaire de la désinformation.* Paris: Armand Colin, 2011, 352 p.

31 SHUKLA, Paurav. « *Essentials of Marketing Research »*, Erie, Ventus Publishing ApS, 2008, 158 p.

32 JEANGÈNE VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina*, op. cit.* note 14, p. 157.

33 *Ibid.*, p. 156.

34 ELDRIDGE, Christopher. HOBBS, Christopher. MORAN, Matthew. « Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data' », *Intelligence and National Security,* Issue 33-3, p. 395.

35 INTELLIGENCE ONLINE. *Criteo embauche un ancien techno de la CIA à Washington*. June 1st 2021.

36 The Mossad is Israel's foreign intelligence service.

37 The Bundesnachrichtendienst (BND) is the German federal government's foreign intelligence service.

38 Covert operations.

39 INTELLIGENCE ONLINE. *Les anciens du Mossad se lancent dans les campagnes électorales en ligne*. August 27th 2021.

40 INTELLIGENCE ONLINE. The DGSE studied tools used by the NSA and the CIA. The agency wants to increase its influence on social media. *Intelligence Online*, n° 797, December 27th 2017, p. 4.

41 *Ibid.*

marketing agencies can also serve strategic purposes. For example, Chinese authorities make extensive use of this approach to exert influence as part of a *soft power* strategy[42].
Consequently, whether the issue is intelligence or marketing, the surveillance of individuals appears to be the point of contention. In 2014, Valérie Peugeot, in her capacity as vice-president of the National Digital Council, argued that the more our economic model relies on digital data to function, the more the infrastructure that makes surveillance technically possible will be put in place. In this context, "*predictive marketing is surveillance's best friend because it collects and processes increasingly detailed data on individuals, which makes surveillance technically possible.*"[43]
Indeed, "*in the age of data, real-time analytics, and predictive analytics, old-school marketing is dead.*"[44]

⁂

In the face of information manipulation, only our individual ability to understand and analyze the mechanisms of falsification can protect us.[45] However, some authors believe that too much confidence is placed in human judgment.[46]
This issue of individual vulnerability, which hinges on individuals taking a critical approach to their relationship with information, actually encompasses an essential social component: making the targeted populations more resilient in order to prevent the fragmentation of national cohesion and the delegitimization of democratic states. In this context, the amplification provided by digital tools "*also poses new risks of alienation for individuals and societies.*"[47]
Ultimately, when it comes to information manipulation, "*state and non-state actors engaged in this activity must bear in mind that there are no passive observers. This is a total war, without front lines, in which there is no such thing as neutrality.*"[48]

Captain Pascal MARTIN is a department head within the National Cyber Unit and holds a Ph.D. in modern and contemporary history.

Translated by Second Lieutenant Joshua JAMES

42 CHARON, Paul. JEANGÈNE VILMER, Jean-Baptiste. *Les opérations d'influence chinoise. Un moment machiavélien*. Report from the Institut de recherche stratégique de l'École militaire (IRSEM), Paris, Ministry of the Armed Forces, 2021, p. 261.
43 MORIN-DESAILLY, Information report prepared on behalf of the fact-finding mission « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », Tome I, n° 696, Sénat, 2014, p. 76.
44 Statement by Jean-Claude Heudin, Director of the Institute for the Internet and Multimedia. In : DE GANAY, Claude, GILLOT, Dominique. *Pour une intelligence artificielle maîtrisée, utile et démystifiée*. Report on behalf of the Parliamentary Office for the Evaluation of Scientific and Technological Choices, tome II, annexe 7, p. 187.
45 See: *Dossier final.* Observatory on (Dis)information & Geopolitics in the Age of COVID-19, edited by François-Bernard HUYGHE and Anne SÉNÉQUIER, Institute for International and Strategic Relations (IRIS), 2021, p. 5.
46 REMANJON, Jérôme, *op. cit.* note 3, p. 4.
47 Jean-Yves Le Drian, Minister for Europe and Foreign Affairs, speech delivered on April 4th, 2018, at the International Conference on Information Manipulation.
48 CANADIAN SECURITY INTELLIGENCE SERVICE, *op. cit.* note 14, p. 30.