Towards a Definition of Cognitive Warfare

Marie Morelle, Cegarra Julien, Damien Marion, André Jean-Marc

Towards a Definition of Cognitive Warfare

MORELLE Marie
Univ. Bordeaux, Bdx INP – ENSC – IMS, THALES LAS France
33400 Talence, FRANCE
mmorelle@ensc.fr

MARION Damien
THALES LAS France, HEAL
33400 Talence, FRANCE
damien.marion@thalesgroup.com

CEGARRA Julien
INU Champollion
81012 Albi Cedex, FRANCE
julien.cegarra@univ-jfc.fr

ANDRÉ Jean-Marc
Univ. Bordeaux, Bdx INP – ENSC – IMS
33400 Talence, FRANCE
jean-marc.andre@ensc.fr

***Abstract*—Cognitive warfare is an emerging concept in the literature, linked to the development of new technologies and of knowledge on cognition, as well as the involvement of public opinion in conflicts. It is currently the subject of debate within NATO. Used to destabilize adversaries or make them "destroy themselves from the inside", it is becoming a major concern, and we need to learn how to detect it and protect ourselves against it. This paper aims to define cognitive warfare, other close concepts and its players, and to outline the issues at stake.**

Keywords—cognitive warfare, influence strategies, destabilization actions, intelligence

I. Introduction

This paper will provide some insights into cognitive warfare, its definition and related concepts. Bernal et al. [3] suggest that modern cognitive warfare emerged during the Cold War: to avoid another destructive open war between superpowers, they set up proxy conflicts, supporting and opposing small countries or armed groups against each other. In this context, numerous actions have been carried out discreetly, notably by the CIA, the FBI and the KGB. Since the 2000s, there has been an increase in destabilization actions [231], particularly by Russia in its attempts to influence elections, propaganda and cyberattacks, notably against the Baltic states, France and the United States, as described by Backes and Swab [1]. Du Cluzel explains that some countries, like Russia and China, are conducting research into neuroscience and technology for medical, social and military purposes, which could also serve as a means of action for cognitive warfare [9]. But it is in the field of economics that the term "cognitive warfare" was first used, to describe the influences and destabilizing actions implemented by companies, towards consumers, legislators (lobbying) or even competing companies [11].

Cognitive warfare thus represents a new mode of conflict blurring the boundaries between war and peace [21], not open warfare on a battlefield, but undeclared warfare aimed at influencing the cognitive mechanisms, notably the decision-making processes, of an adversary or competitor. It's a recent term, and not yet universally accepted. We propose a definition, and discuss the challenges of this new type of confrontation.

II. Cognitive Warfare

Cognitive warfare is an emerging concept aiming to weaken the enemy in order to gain a tactical or strategic advantage [18], in the military, economics, gaming, sports and other fields. It encompasses various operations carried out against the human mind, targeting both individual and collective cognition and decision-making. It can be carried out and suffered at different scales, and remotely: populations, soldiers, experts, engineers, technicians, groups or minorities of opinion, ethnic or religious, companies, communities, decision-makers, political, economic, religious, academic or military leaders [3, 7]…

It relies on NBIC (Nanotechnologies, Biotechnologies, Information technologies and Cognitive sciences) tools, such as digital tools and social networks, chemical substances, illusions, attention saturation [7], or exploitable cognitive biases of targets [22]. The objectives of cognitive warfare can be to conquer a territory, disrupt public services, bring about a change of government, influence elections, undermine confidence, inhibit critical thinking [9], or destabilize and influence a target population [3] by radicalizing opinion, discrediting governing bodies, triggering or inhibiting actions, etc. These actions are difficult to detect, as both targets and relays are unaware that they are victims.

Here are different examples of actions that could be considered as cognitive warfare.

1. Cognitive warfare launched via cyber tools: On the 23rd of February, 2022, just before the Russian offensive against Ukraine, almost 500 cyber-attacks were detected on Ukrainian networks. They targeted essentially the government, critical networks and energy suppliers. According to Malin [17], the goal was seemingly to prevent the Ukrainian government from communicating and providing vital resources to its population, so that they lose confidence in the government. Even though this action is widely considered as cyberwarfare, it can be studied in the perspective of cognitive warfare because it is part of a strategy using different tools with a broader goal of destabilization.
2. Cognitive warfare launched contacting directly key individuals: On the 6th of February 2023 in France, several women deputies from the Rassemblement National received a vocal message telling them one of their children was hospitalized, so that they would leave the National Assembly before a critical vote [24]. This was an intimidation attack trying to prevent the targeted people from voting and thus taking their role in a decision.
3. Cognitive warfare launched on social media: Our last example takes place in Mali, in April 2022. The Wagner mercenary group staged a human mass grave

and edited a video to make it look like the French military created it [14]. The French military managed to film them preparing this staged scene, allowing them to create a video refuting these accusations. According to Jousset and Bolchakova [14], the Wagner group would have used this opportunity to create an influence campaign on social networks to delegitimize the French army in Mali and be welcomed as liberators against French oppression.

4. Another example often used to describe cognitive warfare is the Havana Syndrome [26], which could potentially be a cognitive warfare attack launched using targeted nano or biological tools to induce fear for the key individuals who were targeted and cloud their judgment, but there is no definite cause officially identified, so this example is not supported by evidence to present day.

These examples show how cognitive warfare strategies can be led using different means and channels of action. We propose 3 criteria to help determine whether an action falls within the scope of cognitive warfare:

1. Its purpose is broader than what is immediately apparent: for example, a cyberattack launched in order to steal credit cards and use them to gain a monetary advantage would not be cognitive warfare; but if the aim is to instill doubt in customers' minds about the bank's ability to be secure, and the perpetrator communicates about this to discredit it, this could be an example of cognitive warfare.

2. Its nature is diffuse: it is often part of a strategy encompassing different actions and different means with a goal of chain reactions which can be difficult to measure in time and space. For example, an action could aim at changing behaviors in a population, so another group of people would have a different point of view on this population and then it would have an impact on some votes or decision-makers, and we can imagine a whole chain of resulting consequences and actions; it would thus prove difficult to find the origin of the attack and determine how long-term its effects can be.

3. Its target is cognition: cognitive warfare targets the human mind, representations and cognition, it aims at sowing doubt, preventing or influencing decisions, undermining the opponent's will [21], manipulating the way people see and interpret specific parts of the world around them [3]… In short, how people think and react [25].

III. Close Concepts

There are other concepts closely related to cognitive warfare. We propose a clarification of terminology to better organize and define related terms. Most of them are intertwined with cognitive warfare and/or can be used as tools to lead a cognitive warfare strategy, under the circumstances explained earlier.

A. *Information Warfare, or Information Operations*

NATO[1] describes information warfare as "an operation conducted to gain an informational advantage over the opponent". It focuses on information, its manipulation, its flow, the way it is protected or stolen, and the way it is used. Du Cluzel [20] reminds us that cognitive warfare, on the contrary, is "an action against the way we think, the way we process information and turn it into knowledge". Bernal et al. [3] argue that cognitive warfare is the "fight to control or alter the way people react to information". Intelligence, on the other hand, is a process of knowledge construction [5]. Unlike information warfare, cognitive warfare does not focus on tactical battlefield information, but also acts on information for the general public [3].

B. *Psychological Operations (PsyOps)*

According to Bernal et al. [3], U.S.-led PsyOps involve informational products that are either identifiable as officially U.S.-produced (white products), ambiguously sourced (gray products), or created to "seem as if they originate from a hostile source" (black products). They often have a military purpose. Bernal et al. point out that cognitive warfare works mostly with gray products, which can be denied, and that it "tends to target civilian social infrastructure and governments".

C. *Propaganda*

Propaganda is the transmission of communications, information, and messages for the purpose of causing changes in the consciousness or subconsciousness of the target population, in order to change attitudes and behaviors [4]. Its author assumes authorship, so it is directly attributable. Cognitive warfare is subtler than propaganda. It allows one to influence targets without them being aware of it, and to use these same targets as weapons to reach others. According to du Cluzel [9], with cognitive warfare, "everyone participates, mostly inadvertently, to information processing and knowledge formation in an unprecedented way". The author states that cognitive warfare "feeds on the techniques of disinformation and propaganda aimed at psychologically exhausting the receptors of information": they can therefore be cognitive warfare tools.

D. *Cyber Warfare*

Bernal et al. [3] define cyber warfare as "the use of cyberattacks with the intention of causing harm to a nation's assets". In our connected societies, especially with the Internet of Things, many functions are digitally controlled: "from construction equipment, to financial institutions, to civilian infrastructure, and even to military installations". Thus, cyberattacks can cause "massive damages not just in terms of time and data loss but in physical damage that can be measured in dollars and lives". Computer warfare falls under the technical domain, and the cognitive effect is a consequence, whereas for cognitive warfare, it is the goal of the action [7].

E. *Cyberpsychology*

According to Claverie and Kowalczuk [8], cyberpsychology is the study of mental phenomena in relation to cyber systems and cyber contexts. It is therefore a field of research that

[1] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

could produce knowledge that could be exploited as weapons for cognitive warfare, or, on the contrary, conceive ways of protecting against it.

F. Military Brain Science

According to Jin, Hou, and Wang [12], "Military Brain Science (MBS) is a cutting-edge innovative science […] based on the theories and technologies of medicine […], biology, physics, computer science, military science, and multiple other disciplines". It aims to monitor, protect, fight, repair, improve the brain. These are applications and tools that can be used for cognitive warfare, but remain focused on the military domain.

IV. Targets and Actors

One of the characteristics of Cognitive Warfare is that it can be conducted by anyone, against anyone, and at a distance.

A. Targets

We propose that three kinds of targets can be considered:

1) Large groups of people sharing a common characteristic (populations, opinion, ethnic or religious groups or minorities, etc.);

2) Small groups of people sharing a common goal (companies, teams, armed forces, etc.);

3) Critical individuals (decision-makers, politicians, military leaders or leaders of the various groups mentioned above, experts…);

People who have influence (critical individuals), either on a decision or on a group of people, can be particularly targeted, either directly or indirectly by attacking the large or small group they belong to, which will have repercussions on them (for example, a shift in public opinion can lead to a change of policy or a resignation). Bernal et al. [3] remind us as well that we should not forget "connectors, mavens, and salespeople", who "can be instrumental in the application of cognitive warfare".

As du Cluzel emphasizes, "any user of modern information technologies is a potential target. It targets the whole of a nation's human capital" [9].

B. Actors

Like targets, actors conducting Cognitive Warfare can be varied. Du Cluzel [9] points out that cognitive warfare and the advances in human sciences could potentially confer significant power to anyone who takes the trouble to study them, so that even isolated individuals or small groups can represent a major threat to democracies or military operations.

V. Cognitive Warfare and AI

Artificial Intelligence (AI) is bringing new tools facilitating cognitive warfare, that can amplify it and make it even more accessible and low cost, especially when it comes to fake news and disinformation diffusion.

Du Cluzel reminds us that fake news campaigns combine real and distorted information (misinformation), exaggerated facts and fabricated news (disinformation) [9].

Among these facilitating tools, Mad Scientist Laboratory [16] cites deepfakes, videos generated by artificial intelligence that can show a person reciting a speech he or she never actually gave: their danger is obvious, given that any influential personality can be made to say anything. They can be rendered even more realistic by technologies that imitate the tone of a person's voice and their accent [6]. The risk associated with AI-generated bodies and faces is less obvious, but just as real: it enables the creation of numerous fake accounts on social networks with people who do not exist, and makes it possible to humanize bots to give them more credibility. Generating the face of a person who does not exist is instantaneous, as can be seen at https://thispersondoesnotexist.com/. The last tool cited by Mad Scientist Laboratory is AI text generation, and this tool is brought up to date by the deployment of Chat-GPT in November 2022. This type of tool helps spread false information since it can write articles, posts and comments on social networks much faster and on a larger scale than a team of humans could. Thus, a single group could generate thousands or even millions of comments and posts on social networks, oriented to support or undermine a cause; and these actions would have "the potential to erode the relationship between governments and their citizens, provoking severe reactions throughout the world and leading people to question the very reality they believe" [16]. For example, the Twitter social media is host to many bots, which can "pursue malicious goals such as election interference and extreme propaganda" [10].

An example of the possible application of destabilization campaigns via fake news on social networks is the influence of elections. Russia is particularly active in this field, and "the Kremlin considers disinformation and information operations to be the most effective means of affecting political outcomes in other countries", seizing on "existing domestic political, social, or ethnic divisions and instrumentalizes them to change how voters think – and through that how they vote" [1].

VI. A Few Approaches to Protect Ourselves

Some examples of individual solutions exist against specific cognitive warfare actions. For example, some countermeasures against public influence and fake news on social media were listed: public education, communication about fake news, automatic and human moderation, debunks, legal regulations [1, 13, 27], etc.

Another way for protection and prevention is to use cognitive warfare defensively. Cognitive warfare tools can be used to educate the populations through media and social media [2], enhance cognitive readiness [19] or even augment soldiers' cognition [12]. We could also imagine decision-making tools taking into account cognitive biases and potential cognitive warfare aggressions.

The first step to organize an overall solution is to analyze the opponent and understand how they lead cognitive warfare strategies [21]. This would enable those under attack to be able to detect cognitive warfare offensives early and lift the fog of war [25]. Further research on this topic is necessary in order to build systematic solutions.

VII. Limitations and Criticisms of Cognitive Warfare

Certain destabilizing or influencing actions can be detected and countered: for example, a company implementing a cognitive warfare strategy towards its competitors or customers could be denounced by a data leak or a whistleblower, and this strategy would then backfire by damaging its public image.

Cognitive warfare may also face ethical challenges: it involves influencing the thinking and decision-making of a person or group of people without their knowledge. In this respect, it can be compared to nudges, which encourage the user of a system or tool to behave optimally [15]: it is also a tool of influence, but it is its use that determines its ethical characteristics. Indeed, if the nudge consists in pushing a consumer to buy more or at a higher price, it will be judged more negatively; but if it pushes him or her to behave more respectfully (according to the applicable societal and cultural norms), as with the example of the fly-shaped sticker in the toilet to encourage "better aim", it will be judged more positively. The same applies to cognitive warfare, which must be used in a reasonable and justifiable way.

ACKNOWLEDGMENT

This research is financially supported by the French Ministry of Defence - Defense Innovation Agency (AID).

REFERENCES

[1] O. Backes, and A. Swab, "Cognitive Warfare—The Russian Threat to Election Integrity in the Baltic States". Doctoral dissertation, Harvard University (2019).

[2] B. Battrawi, R. Muhtaseb "The Use of Social Networks as a Tool to Increase Interest in Science and Science Literacy : A Case Study of « Creative Minds »" Facebook Page. (2013).

[3] A. Bernal, C. Carter, I. Singh, K. Cao, and O. Madreperla, "Cognitive Warfare: An Attack on Truth and Thought". NATO and Johns Hopkins University: Baltimore MD, USA (2020).

[4] G.-D. Bobric, "The Overton Window : A Tool for Information Warfare". In J. Lopez, K. Perumalla and A. Siraj, ICCWS 2021 16th International Conference on Cyber Warfare and Security, pp. 20-27 (2021).

[5] F. Bulinge, "Renseignement militaire : une approche épistémologique". Revue internationale d'intelligence économique, 2, pp. 209-232 (2010). https://www.cairn.info/revue--2010-2-page-209.htm

[6] M. Chenouard, "L'intelligence artificielle peut-elle piéger votre mère en imitant votre voix ?" Courrier international. (2023). https://www.courrierinternational.com/video/video-l-intelligence-artificielle-peut-elle-pieger-votre-mere-en-imitant-votre-voix

[7] B. Claverie, B. Prébot, and F. du Cluzel, "Cognitive Warfare : La guerre cognitique". In B. Claverie, B. Prébot and F. du Cluzel (dir.), La Guerre Cognitique, p. 1, CSO (2021).

[8] B. Claverie, and B. Kowalczuk, "Chapitre 9 – Cyberpsychologie". In B. Claverie, B. Prébot & F. du Cluzel (dir.), La Guerre Cognitique, pp. 9.1-9.5, CSO (2021).

[9] F. du Cluzel, "Cognitive Warfare". Innovation Hub (2020).

[10] S. Feng, H. Wan, N. Wang, J. Li, and M. Luo, "TwiBot-20: A Comprehensive Twitter Bot Detection Benchmark". In *Proceedings of the 30th ACM International Conference on Information & Knowledge Management*, 4485-94 (2021). https://doi.org/10.1145/3459637.3482019.

[11] C. Harbulot, "De la légitimité de la guerre cognitive. Revue internationale et stratégique", 56(4), pp. 63 67 (2004).

[12] H. Jin, L.-J. Hou, and Z.-G. Wang, "Military Brain Science – How to influence future wars". Chinese Journal of Traumatology, 21(5), pp. 277-280 (2018). https://doi.org/10.1016/j.cjtee.2018.01.006

[13] Johns Hopkins University & Imperial College London. "Sensibilisation et résilience, les meilleures armes contre la guerre cognitive ". NATO Review, 2021. https://www.nato.int/docu/review/fr/articles/2021/05/20/sensibilisation-et-resilience-les-meilleures-armes-contre-la-guerre-cognitive/index.html#:~:text=Dans%20la%20guerre%20cognitive%2C%20l,mais%20%C3%A9galement%20sur%20leurs%20actes.

[14] A. Jousset, and K. Bolchakova, "Wagner, l'armée de l'ombre de Poutine". Capa Presse (2022).

[15] G. Loewenstein & N. Chater. "Putting Nudges in Perspective". *Behavioural Public Policy* 1, nº 1 (2017): 26-53. https://doi.org/10.1017/bpp.2016.7.

[16] Mad Scientist Laboratory contributors. "149. The Death of Authenticity : New Era Information Warfare." (2019, May 30). https://madsciblog.tradoc.army.mil/149-the-death-of-authenticity-new-era-information-warfare/

[17] I. Malin, "Cyberattaques : comment l'Ukraine a failli perdre la guerre avant même l'invasion russe." (2022, 9 October).

[18] P. Montocchio "Avant-propos par le directeur adjoint du Collaboration Support Office (CSO) STO". In B. Claverie, B. Prébot and F. du Cluzel (dir.), La Guerre Cognitique, pp. vii-viii, CSO (2021).

[19] J. E. Morrison & J. D. Fletcher, "Cognitive Readiness". Institute for Defense Analyses. (2002)

[20] B. Norton, "Behind NATO's 'cognitive warfare': « Battle for your brain » waged by Western militaries". The Grayzone (2021). https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/

[21] K. Orinx, and T. Struye de Swielande, "La guerre cognitive – Pourquoi l'Occident pourrait perdre face à la Chine ?" In B. Claverie, B. Prébot and F. du Cluzel (dir.), La Guerre Cognitique, pp. 8.1-8.7, CSO (2021).

[22] O. Pinard Legry, "Neurosciences et sciences cognitives : Comment se préparer à la guerre des cerveaux ?" Revue Défense Nationale, N° Hors-série(HS3), pp. 58-76 (2022).

[23] J. Prier, "Commanding the trend : Social media as information warfare". In *Information Warfare in the Age of Cyber Conflict*, pp. 88-113, Routledge (2020).

[24] "Réforme des retraites : Des députées RN cibles de messages d'intimidation". Le Monde.fr. (2023, février 7). https://www.lemonde.fr/politique/article/2023/02/07/reforme-des-retraites-des-deputees-rn-cibles-de-messages-d-intimidation_6160845_823448.html

[25] Weldon, A. (2021). *Bytes not bombs : Student team works with NATO to define, track cognitive warfare attacks*. Johns Hopkins University - The Hub. https://hub.jhu.edu/2021/10/06/cognitive-warfare-attacks/

[26] Wikipedia contributors. "Syndrome de La Havane". In Wikipédia (2022). https://fr.wikipedia.org/w/index.php?title=Syndrome_de_La_Havane&oldid=197673790

[27] M. Wunder, "Chapitre 7 – Les narrations submergent le monde". In B. Claverie, B. Prébot and F. Du Cluzel (dir.), *La Guerre Cognitique* (p. 7.1-7.4). CSO (2021).