Revista ARACÊ
ISSN: 2358-2472

COGNITIVE WARFARE ON SOCIAL NETWORKS: THREATS, CHALLENGES AND IMPLICATIONS FOR SOCIETY

https://doi.org/10.56238/arev7n3-240

Date of submission: 24/02/2025 **Date of publication:** 24/03/2025

Vinícius Marques da Silva Ferreira[1], Carlos Alberto Nunes Cosenza[2], Alfredo Nazareno Pereira Boente[3], Kilmer Pereira Boente[4], Renata Miranda Pires Boente[5], Ana Maria dos Santos Vianna[6], Eduardo Luiz Pareto[7] and José Mauro Baptista Bianchi[8]

[1] PhD in Production Engineering
Federal University of Rio de Janeiro, COPPE/UFRJ
E-mail: vinicius.ferreira@pep.ufrj.br
ORCID: https://orcid.org/0000-0003-3664-3510
Lattes: http://lattes.cnpq.br/6490780573139543
[2] PhD Production Engineering
Federal University of Santa Catarina, PPGEP/UFSC
E-mail: cosenza@pep.ufrj.br
ORCID: https://orcid.org/0000-0002-2911-6184
Lattes: http://lattes.cnpq.br/8408511964332556
[3] PhD in Production Engineering
Federal University of Rio de Janeiro, COPPE/UFRJ
E-mail: boente@nce.ufrj.br
ORCID: https://orcid.org/0000-0002-2718-4917
Lattes: http://lattes.cnpq.br/7741044822342404
[4] PhD student in Production Engineering
Federal University of Rio de Janeiro, COPPE/UFRJ
E-mail: kilmerboente@ufrj.br
ORCID: https://orcid.org/0009-0008-6949-9053
Lattes: http://lattes.cnpq.br/4857106401040787
[5] PhD student in History of Sciences and Techniques and Epistemology
Federal University of Rio de Janeiro, HCTE/UFRJ
E-mail: renata@hcte.ufrj.br
ORCID: https://orcid.org/0000-0001-7856-5691
Lattes: http://lattes.cnpq.br/8792693794416432
[6] PhD student in History of Sciences and Techniques and Epistemology
Federal University of Rio de Janeiro, HCTE/UFRJ
E-mail: anamariavianna@ufrj.br
ORCID: https://orcid.org/0000-0002-4126-8682
Lattes: http://lattes.cnpq.br/7378972140573270
[7] Master in Computer Science
Federal University of Rio de Janeiro, NCE/UFRJ
E-mail: epareto@gmail.com
ORCID: https://orcid.org/0009-0001-9854-6663
Lattes: http://lattes.cnpq.br/1558288328722036
[8] Master in Transportation Engineering
Military Engineering Institute, PPGT/IME
E-mail: jose.mauro.bianchi@gmail.com
ORCID: https://orcid.org/0009-0007-2689-411X
Lattes: http://lattes.cnpq.br/2736743448771232

Revista ARACÊ
ISSN: 2358-2472

ABSTRACT
The article analyzes the relevance of digital social networks in the field of Information Science, analyzing their impacts on other spheres of society. In addition to being spaces for interaction and content production, these platforms exert significant influence on the dissemination of information and the construction of contemporary narratives. However, their breadth and reach also make them susceptible to the spread of disinformation and fake news. The research explores fundamental concepts such as Cognitive warfare, hybrid warfare, and narrative warfare, highlighting strategies that combine psychological, communicational, and technological elements to shape perceptions and influence behaviors. These tactics, widely used in political and social contexts, represent growing challenges to democracy, privacy, and digital security. The study adopts a qualitative and quantitative approach, based on a literature review and document analysis, seeking to understand how these phenomena impact society and what strategies can be adopted to mitigate their effects. The results highlight the need for regulatory mechanisms and educational practices that promote critical thinking and information verification, strengthening society's resilience in the face of these new forms of manipulation.

Keywords: Digital social networks. Cognitive warfare. Hybrid warfare. Narrative warfare. Fakenews.

Revista ARACÊ
ISSN: 2358-2472

INTRODUCTION

In fact, it is essential to analyze the conceptual success of digital social networks in light of Information Science, considering their relevance and scientific contribution to research in this contemporary field.

Currently we see that digital social networks lead us to compare their omnipresence and reflect on the increasing occupation of space in academic debates, in the media, in private and public institutions, as well as in social common sense. Therefore, the definition of a network is inherent to human beings, as it is a natural condition and consequently leads them to meet with their neighbors, establishing bonds of friendship, professional relationships, and relationships of interest that extend and change over time. It is possible to see that information and knowledge are present in all spheres, aspects, and areas, considered fundamental from both a professional and academic point of view, when modified by the actions of actors or individuals. Becoming a highly valued skill, enabling socioeconomic growth and development that encourage progress, these being essential resources for the composition and maintenance of digital social networks.

We also know that, by consensus, printed and digital newspapers and publishers are conscientious about publishing daily events and authenticating the spread of news. However, the nature of social media or digital social networks is different from traditional media, as it is dynamic, interactive and allows actors or individuals autonomy to produce content for digital dissemination, but they are not held responsible for the content. Thus, the veracity remains questionable on social media platforms or digital media. However, individuals in traditional media do not have instruments to monitor or control the dissemination of content.

The manifestation of misinformation and the spread of fake news is not a 21st century event. When analyzing social historical periods in the world, we can see that such an event is inherent to human communication, since the phenomenon of these channels, through printed newspapers, radio and television, were already held responsible for causing the effect of misinformation when they became popular. In the 20th century, with the introduction of the Internet, the speed of information propagation further increased the speed at which reports multiply, compromising the verification of sources and the reliability of facts, which foster an environment in which the feeling of “anonymity or concealment” on social networks allows for the promotion of herd-like social behavior, spreading news without verification.

Revista ARACÊ
ISSN: 2358-2472

According to Rais (2018), the concept of fake news is based on three essential elements: intent, falsehood, and damages. However, we often have to deal with data and information that naturally cannot be specified by precise numerical values and, in addition, it is necessary to have the ability to analyze them in order to make decisions or conduct a case study more accurately. This information, despite being scalable, involves a certain degree of interpretation and actions driven by subjectivity, that is, it admits disagreements between individuals in a group, ambiguities, inconsistencies, relativizations, uncertainties, and the influence of socioeconomic and cultural values, incurring collective effects on networks that reveal internal and external divergences.

The growing relevance of digital social networks in contemporary society has revisited a series of challenges related to the dissemination of information and the construction of narratives. In this context, concepts such as Cognitive warfare, hybrid warfare and narrative warfare have emerged, with a significant impact on social and political dynamics, since Cognitive warfare, hybrid warfare and narrative warfare are related concepts, but have different emphases and approaches in the context of contemporary conflicts.

Cognitive warfare, hybrid warfare, and narrative warfare are complex phenomena that have been growing in recent decades, driven by the intersection of science, technology, and society. These terms describe conflict strategies that go beyond traditional approaches to warfare, incorporating elements of psychology, communication, technology, and cybernetics to influence people's opinions, beliefs, and behaviors. The use of these strategies on social media has become particularly evident and worrying.

METHODOLOGY

This study considers a qualitative approach, focused on the analysis of documents and bibliographic sources, with the aim of investigating the dynamics and implications of Cognitive warfare on social media, particularly in relation to threats, challenges and implications for society. The research uses as an example and starts from a detailed examination of the manipulation and influence tactics used by the governments of Russia and China on digital social media, as well as the implications of the bilateral agreement signed between these two countries on February 4, 2022, which established multipolarity as a new global geopolitical positioning (Jochheim, 2022).

Revista ARACÊ
ISSN: 2358-2472

In addition, the study examines how states and other strategic actors use information as a tool of power and influence, aiming to provide guidelines for military planning and prepare defense institutions for future events, thus ensuring a strategic advantage in possible conflicts. The analysis also covers the role of non-state actors, such as Cambridge Analytica, which used advertising strategies targeted at Facebook users for political purposes, in order to better understand the dynamics of cognitive operations in the context of hybrid wars.

To carry out the analysis, secondary sources were used, such as academic articles, books, reports from research institutions and official documents, aiming to develop a broad overview of the tactics and strategies applied in Cognitive warfare on social networks.

COGNITIVE WARFARE ON SOCIAL NETWORKS AND ITS CONSEQUENCES IN THE DIGITAL CONTEXT

Cognitive warfare on social media represents a virtual battlefield where information is used strategically to influence perceptions and behaviors, shaping the digital landscape in favor of certain actors, be they states, organizations or individuals. This phenomenon has been expanded with technological advances and the ubiquity of digital platforms, causing significant implications for society, politics and security.

The manipulation of information on social media, by distorting reality and spreading false narratives, has significant social consequences. This phenomenon influences public opinion, intensifies social divisions and compromises public debate, affecting the democratic process and favoring radicalization and polarization.

Figure 1 - Cognitive Warfare on Social Media.

Source: DALL-E, 2025.

Revista ARACÊ
ISSN: 2358-2472

In the political sphere, social networks have become strategic arenas for political disputes, with Cognitive warfare being used as a tool to interfere in elections, manipulate political agendas and destabilize governments. Examples include the use of fakes profiles, bots and disinformation campaigns that aim to shape voters' perceptions, influence their votes and, consequently, electoral results.

Furthermore, in the context of security, the use of Cognitive warfare as a tool on social networks can be used to disseminate false information that compromises national security, as in the case of fake news that aims to discredit defense and security institutions, since the manipulation of information can also be used as a strategy to sow chaos, destabilize societies and achieve geopolitical objectives.

Modernity has provided broad digital integration, connecting people in a global network of information and social interactions. However, this virtual environment has also become a cognitive battlefield, where various actors seek to influence perceptions and behaviors to achieve their objectives. Cognitive warfare on social media, waged by nations such as Russia and China, as well as private actors such as Cambridge Analytica, poses a significant threat to democracy, privacy and security in the digital space.

Russia's tradition of wielding power and influence, as demonstrated by its social media operations during the 2016 US presidential election, seeks to undermine the US-led global order and favor candidates aligned with its geopolitical interests (ICA, 2017). According to NATO (2021), Russia's National Security Strategy, signed by Vladimir Putin in 2021, presents a vision of an interconnected world in which battlefields extend to both the internal and external environments of states.

At the same time, China is seeking to improve its capabilities in cyber warfare, electronic warfare and psychological warfare through a strategy of "informatization" of its armed forces. The integration of advances in brain science, artificial intelligence and biotechnology aims to strengthen Chinese military power in the face of the increasing complexity of military operations (Xinhua, 2017; Hangui, 2016).

Cognitive warfare is characterized using information and misinformation to shape opinions, beliefs, perceptions and behaviors. The Cambridge Analytica case in the 2016 US elections is an emblematic example, where private data from Facebook users was used to influence the vote in favor of Donald Trump (Claverie and Du Cluzel, 2022).

The implications of Cognitive warfare on social networks are profound and require a coordinated response between governments, technology companies and civil society, as

Revista ARACÊ
ISSN: 2358-2472

well as the preservation of the integrity of the digital space and the protection of the fundamental values of democracy are imperative in the face of this complex and impactful phenomenon.

The United Nations (UN) has taken a stance on this challenge, as exemplified by the Declaration on Freedom of Expression, Fake News, Disinformation and Advertising (OSCE, 2017). This declaration reaffirms the need for a joint effort between various actors, including intermediaries, the media, civil society and academy, to understand and combat disinformation. Furthermore, the document disapproves of attempts by some States to impose restrictions and controls on digital technologies and pressure third parties to adopt content-restrictive measures.

Cognitive warfare on social media is, therefore, a complex and challenging phenomenon that requires coordinated and integrated action by various actors to mitigate its negative impacts and preserve democratic values and the integrity of the digital space. The responsibility lies with governments, technology companies, civil society and international organizations, which must work together to face this challenge and protect the fundamental rights of citizens in the digital age.

To address this phenomenon, a multidisciplinary approach is needed that involves cooperation between governments, technology companies, civil society and academy. Essential measures include promoting digital education and media literacy, implementing fact-checking mechanisms, regulating algorithms and improving cybersecurity.

COGNITIVE WARFARE VS HYBRID WARFARE

To avoid traditional warfare and military deployments, the battlefield and the way of fighting have changed since the end of World War II. In fact, Cognitive warfare and hybrid warfare are two concepts that relate to modern, unconventional forms of conflict, but have different approaches. Here is a comparison of these two concepts:

Hybrid warfare refers to complex combinations of conventional, irregular, and terrorist conflicts, as well as actions that can be carried out by state and non-state actors, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion, as well as criminal disorder. These combined actions exploit adversary vulnerabilities. The abstractness of the term means that it is used as a generic term for all non-linear threats.

Revista ARACÊ
ISSN: 2358-2472

A hybrid adversary may also use covert actions to avoid attribution or retribution. The methods are used simultaneously across the spectrum of conflict with a unified strategy. It is often used to confuse and disrupt adversary decision-making.

Cognitive warfare is a strategy that focuses on changing how a target audience thinks and in turn changing how they will act. From a military perspective, destabilizing and influencing the target audience are fundamental objectives, since this fact leads us to conclude that Cognitive warfare focuses on manipulating human perception and thought to achieve strategic objectives. This can be done through disinformation, advertising, psychological influence and cyber operations that affect the way people perceive and understand reality. Cognitive warfare seeks to control the brain and thoughts, aiming to change behavior, as the unconventional means uses cyber tools to alter the adversary's cognitive process, exploiting mental biases or reflexive thoughts to provoke thought distortions, influencing decision-making, preventing actions with negative effects, both at the individual and collective levels.

Figure 2 - Cognitive Warfare vs Hybrid Warfare.

Source: DALL-E, 2025.

Revista ARACÊ
ISSN: 2358-2472

The concept of Cognitive warfare can be seen as a combination of the newest cyber techniques associated with information warfare and the more human-friendly components together with the manipulative aspects of psychological operations. It generally involves a biased presentation of reality, often digitally altered, to favor one's own interests. New communication tools now offer endless possibilities, opening the way for new methods and new objectives.

Cognitive warfare can be understood as an integral part of hybrid warfare, influencing its strategies. However, it also has its own characteristics that allow it to occur independently. Its impact can be felt even without the presence of other elements of hybrid conflict.

STRATEGIES AND TACTICS OF COGNITIVE WARFARE

According to Ferreira (2024, pp. 10), Cognitive warfare is a form of conflict that focuses on the use and manipulation of information with the aim of influencing the perception and behavior of individuals, groups and organizations, because unlike traditional warfare, which primarily aims at physical destruction or territorial conquest, cognitive warfare aims to obtain a strategic advantage by affecting the minds of opponents, altering their decisions and actions, in other words, it aims to change people's ways of acting, and this is a fundamental difference in relation to previous wars.

Table 1 - Instruments of Cognitive Warfare.

Topics	Descriptions
Advertising and Selective Information	One of the oldest instruments of cognitive warfare is advertising. Information is carefully selected and distributed to influence the masses, promote an agenda, or discredit the enemy. Advertising can be disseminated through a variety of means, including traditional media, social media, pamphlets, and even education.
Disinformation and Fake News	The intentional dissemination of false or misleading information is used to create confusion, disorient the population or opponents, and influence public opinion. Fake news is a modern example of this practice, enhanced by the speed and reach of social media.
Cyberattacks	Cyberattacks can be used to steal information, conduct espionage, disrupt communications, or even manipulate data and systems. Such attacks can have direct and immediate effects or long-term consequences on perception and decision-making.
Psychological Warfare	Psychological warfare involves the use of psychological techniques to influence the morale and behavior of an adversary. This may include actions such as distributing demoralizing information or executing operations aimed at exacerbating fear and uncertainty.

Revista ARACÊ
ISSN: 2358-2472

Influence Operations	These are operations designed to change perceptions and attitudes. They can be carried out in more subtle and strategic ways, often through agents of influence, public relations and diplomacy.
Narrative Control	Controlling narratives is key to cognitive warfare. This means controlling the story that is told, whether it's about a conflict, a policy, or a nation. Those who control the narrative can shape the perception of reality.
Education and Training	Education can be seen both as an instrument of cognitive warfare and as a means of defense against it. Educational programs and training can be used to strengthen cognitive resilience against external influence.

Source: Adapted from Ferreira, 2024.

Cognitive warfare is changing the way we wage war. Disputes for power are no longer focused on military force, but on developing new techniques and new terrains. The human mind is now considered the new domain of warfare. This is due to the changing nature of warfare, where information warfare, cyber warfare, psychological operations and lawfare are becoming increasingly important.

Psychological influence over the enemy has proven to be more effective than physical attacks or losses on the battlefield. The goal of informational attacks is to shape the opinions, beliefs, perceptions and behaviors of the target audience. Through information and disinformation, the aim is to modify people's psychological state and thus influence the outcome of conflicts.

According to the Brazilian Agency (2019), in 2019, the Chamber of Deputies and the Senate conducted a survey to understand how Brazilians receive information. It was revealed that 79% of Brazilians use whatsapp as a source of information. The number of people who consult major news portals to verify the veracity of information is less than half (38%). TV channels are consulted by only 50% of the population, 44% of Brazilians use facebook as a source of information, far ahead of news portals, which only have 38%, Instagram has 30%, radio 22%, printed newspapers 8% and X 7%, closing the relevant media.

Understanding that the goal of social networks is to keep all the user's attention on their platform, content presentation algorithms feed back to the individual with relevant information that pleases them. This creates an information bubble that distorts realities and increasingly isolates individuals from critical thinking, bringing together people who think the same way and ratifying behaviors. This is the perfect scenario to create an effective Cognitive warfare strategy, which can be used to obtain commercial, political or social engagement advantages (Chen, Chen and Xia, 2022).

Revista ARACÊ
ISSN: 2358-2472

Chinese researchers define this behavior as “social media weaponization,” a phenomenon in which digital platforms are used strategically to influence, manipulate, and even direct public opinion. This militarized use of social media transforms them into powerful tools for political ends, making information not just a form of communication but also an instrument of control and influence in a Cognitive warfare environment.

COGNITIVE WARFARE AS A GEOPOLITICAL STRATEGY

Cognitive warfare emerges as a long-term geopolitical strategy that aims to influence the political sphere and generate lasting impacts on society. This strategy, which differs from psychological operations in that it does not necessarily focus on the quality of information, primarily seeks the desired result, regardless of the veracity of the information used. In this sense, Cognitive warfare can involve document leaks and heated debates on social media, provoking reflections on individual cognitive capacity amid contemporary information overload (Reis, 2019).

One of the central objectives of Cognitive warfare is to undermine public trust in various institutions and processes that are fundamental to democracy and the functioning of society. This includes trust in electoral processes, government institutions, politicians, and allied forces. The quest to destabilize governments through partially true information, promoting discord, and celebrating hatred between classes, is a striking characteristic of this strategy (Silva, 2021).

According to Martins (2020), legal guarantees, by protecting citizens' fundamental rights, can be seen as a benefit for criminal organizations, raising questions about the credibility of public security operators and causing widespread discouragement. This scenario can be used as a component of Cognitive warfare to destabilize public order and question the effectiveness of security institutions.

Another crucial component in this scenario is the "Spiral of Silence", a concept proposed by Elisabeth Noelle-Neumann in the 1960. This term refers to the process by which people's behavior generates a progressive escalation towards silence, especially in polarized environments, such as elections. In this context, social networks increase the prevalence of extremist and aggressive rhetoric, which rejects dialogue and sows’ hatred, stifling dissenting voices and promoting a progressive silencing of other perspectives (Noelle-Neumann, 1974).

Revista ARACÊ
ISSN: 2358-2472

Given this scenario, it is essential to develop strategies and public policies that aim to strengthen society's resilience in the face of these Cognitive warfare tactics, ensuring the preservation of democratic values and trust in institutions that are fundamental to the functioning of society.

CHALLENGES AND INITIATIVES AGAINST COGNITIVE WARFARE

Social media currently plays a central role in conducting Cognitive warfare operations, being used as strategic instruments to shape public opinion according to specific interests, whether political or economic in nature. Through the widespread dissemination of information and narratives, these platforms enable the manipulation of public discourse and the formation of perceptions that favor certain groups or ideologies. In this context, several initiatives have been implemented globally with the aim of reducing the negative impacts of disinformation and targeted advertising. These actions seek to strengthen the veracity of information and promote a more balanced digital environment, mitigating the risks associated with cognitive manipulation on a massive scale.

Table 2 - Challenges Against Cognitive Warfare on Social Media.

Disinformation and Fake News	Social media platforms serve as stages for spreading false or misleading information, which can be used as weapons in Cognitive warfare.
Algorithm Manipulation	The manipulation of algorithms to promote certain narratives or suppress others is a common tactic in Cognitive warfare operations.
Cyber Attacks	Social media platforms are targets of cyber attacks aimed at compromising information integrity and influencing public opinion.
Polarization and Extremism	Cognitive warfare can exploit and amplify societal divisions, fostering polarization and extremism.
Ethical and Legal Challenges	The fight against Cognitive warfare on social media raises ethical and legal issues related to privacy, freedom of expression, and content regulation.

Source: Own elaboration.

Table 3 - Initiatives Against Cognitive Warfare on Social Media.

Education and Media Literacy	Promote digital education and media literacy so that users can identify and resist disinformation.
Fact-Checking and Verification of Information	Implement and strengthen fact-checking mechanisms to combat the spread of fake news.
Transparency and Algorithm Regulation	Demand transparency and regulation of social media algorithms to prevent manipulations that favor certain narratives.

Revista ARACÊ
ISSN: 2358-2472

International Cooperation	Establish cooperation among countries, international organizations, technology companies, and civil society to combat Cognitive warfare on social media.
Enhancing Cybersecurity	Invest in cybersecurity to protect social media from attacks aimed at compromising information integrity.

Source: Own elaboration.

In this context, the United Nations (UN) promulgated the Declaration on Freedom of Expression, Fake News, Disinformation and Advertising, as an effort to establish guidelines that guide the actions of different social actors in combating disinformation (OSCE, 2017). The document is emphatic in encouraging cooperation between intermediaries, the media, civil society and academy in the search for effective strategies to combat fake news and misleading advertising.

According to the Declaration, it is imperative that States do not use restrictive or controlling practices over digital technologies, such as blocking, filtering, obstructing and closing down digital spaces, or exert pressure on third parties to implement content-restrictive measures. Furthermore, it establishes that State actors must refrain from sponsoring, encouraging or disseminating information that they know, or should reasonably know, to be false (disinformation) or that demonstrates a reckless disregard for verifiable information (advertising).

The Declaration also highlights the importance of restrictions on freedom of expression under the justification of protecting national security - such as combating terrorism, extremism and incitement to hatred - being subject to judicial oversight and drafted in a clear and restricted manner. Furthermore, it urges the media and online platforms, referred to as “powerful corporate actors”, to adopt practices that respect human rights, implement fact-checking codes, establish self-regulatory systems and provide tools that enable the identification of content creators, without exerting undue influence over journalistic work (OSCE, 2017).

According to OSCE (2017), thus, the Declaration on Freedom of Expression, Fake News, Disinformation and Advertising is a fundamental document to guide the actions of different social actors in the search for effective strategies to combat disinformation and advertising, thus contributing to safeguarding the integrity of the digital public space and, consequently, to preserving democracy and the fundamental values of society.

Other paths are also being taken. To combat what is happening in the new battlefield, the democratic world has established agreements between courts, such as the

Revista ARACÊ
ISSN: 2358-2472

one between the Superior Electoral Court and social media platforms. Knowing that social media environments are conducive to fostering different tactics for deception, disinformation, advertising, threats to opponents, mobilization of supporters and coordination of actions, such agreements are guides to combat hostile activities on social media and in the information environment. Its actors do not observe the same democratic rules and values (Tribunal, 2022).

A vital way to minimize psychological operations is to raise awareness among citizens and authorities about these activities. According to Liden et al. (2021), they propose four solutions to the problem: algorithmic, corrective, legislative and psychological. The news-generating algorithms for users of social networks such as Facebook, Instagram and X must be able to quickly identify fake news and remove it from circulation. In the corrective solution, the information must be quickly corrected and reach the final recipients quickly. In the legislative solution, laws need to be changed. Finally, in the psychological solution, the so-called psychological inoculation is proposed. This solution is associated with the creation of vaccine mechanisms, developing mechanisms in people to develop a critical sense averse to fake news. It would be a vaccine against brainwashing.

Inoculation can be understood as a solution divided into two main components (Linden et al., 2021). The first consists of a warning to the recipients of the message that false information will arrive. This is said to be the affective basis of the mechanism, as people do not like to be deceived and are alert to this possibility. The second consists of refutational preemption (prebunking). This is said to be the cognitive basis of the mechanism, as when exposed in advance to arguments that refute the threat, the person has a greater cognitive capacity to understand whether the threat reveals itself as false or true information more easily.

CONCLUSION

The article highlights the growing relevance of digital social networks in today's society, not only as tools for interaction, but as essential spaces for the production and dissemination of information. Such platforms have become strategic fields for the development of new forms of conflict, such as Cognitive warfare, hybrid warfare and narrative warfare, which exploit, in an increasingly sophisticated way, psychological, communicational and technological aspects to shape public perception and manipulate

Revista ARACÊ
ISSN: 2358-2472

behavior. This scenario presents significant risks to democracy, privacy and security in the digital space, and is a potential threat to the free and fair functioning of society.

The research also emphasizes the urgency of a comprehensive approach to addressing these challenges. To this end, collaboration between different sectors, including governments, technology companies, civil society and academy, is essential in building solutions that help mitigate the negative impacts of this invisible war on social media. Implementing strategies for fact-checking, regulating algorithms and strengthening cybersecurity are fundamental actions that need to be adopted in a coordinated manner. In addition, digital education must be a priority, enabling individuals to discern false or manipulated information, creating a more critical society that is less vulnerable to these forms of manipulation.

In this context, the actions of global organizations, such as the United Nations (UN), are essential to promote guidelines and public policies that combat disinformation and seek to strengthen society's resilience in the face of cognitive warfare tactics. The UN, together with other international actors, has the responsibility of guiding countries in building a safer, more transparent and ethical digital environment. Digital social re-education thus becomes an essential element in creating a society that is more aware of its online interactions, ensuring that digital platforms are used for the common good and not as instruments of manipulation and disinformation.

Revista ARACÊ
ISSN: 2358-2472

REFERENCES

1. AGÊNCIA BRASIL. **WhatsApp é principal fonte de informação do brasileiro**. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-12/whatsapp-e-principal-fonte-de-informacao-do-brasileiro-diz-pesquisa>. Retrieved on November 2, 2024.

2. CHEN, L.; CHEN, J.; XIA, C. Social network behavior and public opinion manipulation. **Journal of Information Security and Applications**, v. 64, fev. 2022, p. 1-15, p. 1. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S2214212621002441>. Retrieved on October 20, 2024.

3. CLAVERIE, B.; DU CLUZEL, F. **Cognitive warfare: the advent of the concept of cognitics in the field of warfare**. NATO Collaboration Support Office, 2022. Available at: <https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare>. Retrieved on October 15, 2024.

4. FERREIRA, V.M.S. **Lógica Fuzzy Aplicada a Análise Comportamental e Conhecimento da Guerra Cognitiva em Redes Sociais**: Um modelo de extração e mineração de dados. Tese (Doutorado em Engenharia de Produção). Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal do Rio de Janeiro, COPPE/UFRJ, Rio de Janeiro, RJ, 2024.

5. HANGUI, C. **Artificial Intelligence**: disruptively changing the rules of the game. China Military Online, 2016. Available at: <http://www.81.cn/jskj/2016-03/18/content_6966873_2.htm.>. Retrieved on October 12, 2024.

6. INTELLIGENCE COMMUNITY ASSESSMENT (ICA). **Assessing russian activities and intentions in recent US elections**. 2017. Available at: <https://www.dni.gov/files/documents/ICA_2017_01.pdf>. Retrieved on November 1, 2024.

7. JOCHHEIM, U. **China-Russia relations**: A quantum leap?. European Parliamentary Research Service. Available at: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729349/EPRS_BRI(2022)729349_EN.pdf>, p. 1-10, Maio 2022. Retrieved on February 19, 2025.

8. MARTINS, L. Segurança Pública e Organizações Criminosas: Uma Análise do Garantismo Jurídico no Brasil. **Revista Brasileira de Segurança Pública**, vol. 14, nº 3, 2020, pp. 12-28.

9. NATO DEFENSE COLLEGE (NATO). **Russia's updated National Security Strategy**. Available at: <https://www.ndc.nato.int/research/research.php?icode=704>. Retrieved on January 11, 2025.

Revista ARACÊ
ISSN: 2358-2472

10. NOELLE-NEUMANN, E. The Spiral of Silence: A Theory of Public Opinion. **Journal of Communication**, vol. 24, nº 2, 1974, pp. 43-51.

11. ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE). **Joint declaration on media independence and diversity in the digital age**. EUA: UNHR, 2017. Available at: <https://www.osce.org/files/f/documents/1/e/379351.pdf>. Retrieved on November 1, 2024.

12. RAIS, D. Desinformação no contexto democrático. In: **ABBOUD, Georges; JR, Nelson Nery; RICARDO, Campos (Eds.). Fake news e Regulação**. São Paulo. p. 147– 166, ano 2018.

13. REIS, J. A Guerra Cognitiva e a Desinformação no Mundo Contemporâneo. **Revista de Estudos Políticos**, vol. 12, nº 1, 2019, pp. 234-249.

14. SILVA, A. Desestabilização Governamental e Guerra Cognitiva: Uma Análise da Influência das Fake News na Política. **Anais do Congresso Internacional de Ciência Política**, 2021.

15. LINDEN, S.V.D. et al. How can psychological science help counter the spread of fake news?, **The Spanish journal of psychology**, v. 24, n. e25, 2021.

16. XINHUA, W. **Scientific and technological innovation, a powerful engine for the world-class military**. 2017. Available at: <http://www.gov.cn/xin-wen/2017-09/15/content_5225216.htm>. Retrieved on March 10, 2025.