DOI: 10.53477/2784-2487-24-08

MANIPULATING PERCEPTIONS AND BEHAVIOR THROUGH COGNITIVE WARFARE TECHNIQUES IN THE DIGITAL AGE

Lieutenant-colonel Florin-Marius GÎNDILĂ*

Abstract: *Dominated by technology and information in our digital era, cognitive warfare has become a ubiquitous occurrence impacting views and human behavior by leveraging cognitive weaknesses. Rapid spread of propaganda and false information made possible by the Internet and social media seriously influences democracies, economics, and social stability by means of their effects on Emphasizing the need of preserving cognitive integrity, this book investigates how psychology and technology interact to control minds and behaviors. Propaganda, contrived stories, behavioral psychology, and the application of personal data for tailored influence efforts are among the strategies applied. Media education, digital literacy, and the development of psychological resilience are therefore absolutely crucial in order to offset these consequences.*

Keywords: *technology and information; the Internet; Propaganda; social stability; influences democracies.*

Introduction

The technologically driven society of today regularly witnesses the manipulation of ideas and human behavior by means of cognitive warfare techniques. The Internet and social networks have completely changed the way knowledge is shared and absorbed, so generating amazing chances to change public opinion. In this sense, cognitive warfare now covers all spheres of social, political, and economic life, transcending military battles. Given its major impact on democracies, economies, and social stability, it is abundantly evident that research of this phenomenon is important. Studying this subject will enable one to have a complete look at the ways in which psychology and technology interact to influence ideas and behavior. It underlines the need of preserving cognitive well-being in a society going more and more technologically advanced.

1. Conceptual delimitations.

Cognitive warfare is a developing form of conflict that seeks to manipulate and dominate the thoughts, beliefs, and decision-making processes of individuals and groups by exploiting their cognitive vulnerabilities. This method combines modern technologies and knowledge from neuroscience, psychology, and behavioral sciences to subtly and convincingly influence human consciousness, so transcending the traditional boundaries of informational and psychological warfare. NATO's Strategic Communications Center of Excellence defines cognitive warfare as "strategies and tactics designed to influence and manipulate the perceptions, beliefs, and decision-making processes of individuals or groups by exploiting cognitive vulnerabilities. Unlike traditional warfare, which focuses on physical confrontations, cognitive warfare targets the mind, aiming to alter the way people think, perceive reality, and make decisions." (StratCOM COE 2020) Using small and consistent strategies, the main goal of cognitive warfare is to change attitudes and behaviors; this might not always be clear to the affected parties.

Information war "aims at controlling and manipulating information to influence the decisions and actions of the adversary." says Martin Libicki (Libicki 1995) With an aim of erasing the dependability and availability of information, information warfare consists in a spectrum of operations including deception, propaganda, censorship, and cyber-attacks. The main objective of information warfare is to twist and distort the truth so as to shape public narratives and forward the agenda of people in charge of distributing the resources. Cognitive warfare and information warfare differ primarily in their inherent goals and features, even if they have certain similarities. Although cognitive warfare depends on the effect of information on an individual's mental processes, such changes in perception and cognition, information warfare stresses on the content of knowledge and its distribution.

[*] PhD Candidate at the "Carol I" National Defense University, Romania; e-mail: florin_gindila@yahoo.com.

Psychological warfare is the application of psychological methods meant to discredit, threaten, or disrupt an enemy. These strategies use pressure to alter attitudes and behavior and cover the dissemination of messages meant to cause panic, uncertainty, and bewilderment, so inspiring a feeling of powerlessness. Particularly psychological warfare seeks to regulate the emotions and psyche of people or groups so lowering their capacity for resistance and their will to take part in conflict. Renowned authority in the field of foreign policy and national security issues and a major player in the evolution of modern psychological warfare theory, Paul Linebarger defined it "the deliberate use of propaganda and other psychological maneuvers to shape the viewpoints, emotions, attitudes, and conduct of adversary factions."(Linebarger 2015).

Unlike psychological warfare and information warfare, **cognitive warfare** stresses less on the direct transmission of messages and more on indirectly influencing the way people absorb knowledge and grow in their beliefs. Basically, it is about guiding the information flow and the mental framework people build to produce opinions. Moreover, cognitive warfare emphasizes cognitive comprehension and information assimilation over a long period of time, so transcending the control of instantaneous emotional reactions. With the intention of progressively and regularly altering perceptions and behaviors, this calls for a great knowledge of cognitive mechanisms as well as a sophisticated and complex approach.

2. Tools and Techniques Used in Cognitive Warfare

Technology and security specialist P.W. Singer says "modern digital tools provide unprecedented opportunities to influence and manipulate human thinking on an unparalleled scale and depth." (Singer and Brooking 2018) Cognitive warfare customizes and maximizes influence efforts by using advanced technologies and a wide range of tools and tactics. These technologies enable the identification and use of some cognitive flaws in people and groups, so customizing messages to fit the emotional and cognitive inclination of the target audience. Another important element is the use of social networks and other digital platforms to distribute and improve communications in a way that seems natural and reliable. This phenomenon increases its influence on people's views and behavior since it creates a false sense of genuineness and consensus.

Among the earliest and most researched strategies for changing public opinion and behavior is **propaganda**. It means the intentional sharing of knowledge, ideas, or rumors meant to either support or compromise a cause, group, or person. In cognitive warfare, propaganda is used to create and reinforce attitudes and beliefs consistent with the goals of the disseminator. Jacques Ellul defines propaganda "a technique of influence that seeks to change opinions and behaviors by acting directly on the mental representations of individuals," (Ellul 1965) Modern propaganda makes advantage of digital platforms and social networks to target particular groups of people, using sophisticated techniques of tailoring and distribution of information. To grab viewers' attention and set off strong emotional responses, this can include interesting emotional messages, startling images, and simple storylines.

Another essential tool in cognitive warfare is **manipulated narratives**. Joseph Nye says "narratives are powerful because they give our world meaning and structure, so impacting how we view and respond to information." (Nye 2009). These exercises involve the development and spread of stories and ideas that distort the truth and so shape people's perception of events and actions. Stories under manipulation help to shape opinions and create a particular understanding of complex events. Within the framework of cognitive warfare, these stories usually fit the target's current perspective and cultural standards, so simplifying their acceptance.

Cognitive warfare also depends on **behavioral psychology** since it uses strategies of behavior modification grounded in knowledge of how people react to specific stimuli. Without explicit compulsion, techniques including conditioning, nudging, and framing are used to shape decisions and behaviors. Richard Thaler and Cass Sunstein first presented the idea of "nudge," in their book "Nudge: Improving Decisions About Health, Wealth, and Happiness," outlining how small changes in the way options are presented might have a big impact on behavior. (Thaler and Sunstein 2008). Often without the targets conscious of the impact being applied upon them, these strategies are used in cognitive warfare to control actions towards specific objectives.

The utilization of personal data is one of the very effective weapons in the armory of cognitive warfare. Data acquired from digital channels, social media, and other online sources helps one to fully understand personal preferences, behavior, and cognitive susceptibilities. This information helps create and distribute designed and potent communications. In "The Age of Surveillance Capitalism," Shoshana Zuboff writes on how governments and businesses enabled by the vast gathering and analysis of personal data have unparalleled influence over individuals' behavior (Zuboff 2019). Cognitive warfare looks for cognitive flaws using these methods and customizes influence campaigns to increase their effectiveness and persuasiveness.

Advanced technologies including artificial intelligence and machine learning are absolutely required in cognitive warfare since they automate and improve influence operations. Using artificial intelligence and machine learning to analyze vast amounts of data and find trends and patterns helps one to apply these ideas in influence projects. In "LikeWar: The Weaponization of Social Media," P.W. Singer and Emerson T. Brooking call attention to how algorithms dramatically alter the visibility and interpretation of content on social media platforms, so rendering them venues of influence (Singer and Brooking 2018). Depending on the responses and actions of the intended audience, these technologies magnify the impact of messages and change them in real-time, so allowing the execution of cognitive warfare with hitherto unheard-of accuracy and efficacy.

3. Social networks and digital platforms

Both of them have evolved into essential tools in cognitive warfare since they enable the quick and efficient dissemination of manipulative knowledge all around the globe. These platforms provide not only simple access to a big audience but also sophisticated tools for customizing and improving communications, so optimizing their impact on people's opinions and actions. Manipulative messages, false information, and propaganda are distributed widely on well-known social media sites including Facebook, X (Twitter), Instagram, and TikTok. These platforms let players of cognitive warfare quickly create and disseminate viral material with the power to change public perspective."Social networks have become primary channels for manipulating public opinion through the spread of disinformation and false narratives." claims a report by the Oxford Internet Institute (Bradshaw and Howard 2019). These platforms' algorithms are designed especially to maximize user involvement; thus they give content that causes strong reactions top priority—positive or negative. This creates an environment that is ideal for the spread of emotive and divisive messages, which are more likely to be shared generally and go viral

Moreover, a very important factor of using social media in cognitive warfare is the capacity to **customize messages** to fit particular preferences and susceptibilities of individual users. By compiling and analyzing personal data to create thorough profiles of their targets, cognitive warfare actors can produce quite accurate message personalizing. In "The Age of Surveillance Capitalism," Shoshana Zuboff emphasizes "the massive collection of personal data enables not only the anticipation of behavior but also its subtle and unnoticed influence."(Zuboff 2019). This enables the performers to create not only persuasive but also flexible influence campaigns able to change in real time depending on consumer reactions and behaviors.

Furthermore, social networks help to quickly spread manipulative messages, which can be further enhanced by means of bot networks, fake accounts, and coordinated amplification techniques. These approaches can give the impression of general consensus or strong public endorsement for particular ideas or stories. Regarding research by the Atlantic Council "the use of bot networks and fake accounts to amplify manipulative messages can alter perceptions of public opinion and influence behaviors and political decisions." (Alina Polyakova 2019). This is part of a more all-encompassing strategy meant to change impressions and discredit democratic nations by purposefully creating uncertainty and confusion.

Within this field of knowledge, there is debate about the psychology of social networks—which are purposefully designed to exploit consumers' emotional and cognitive weaknesses. Features like "like," "share," and "comment" are meant to set off dopamine release and encourage addictive behavior, so increasing users' vulnerability to outside influences. In "Persuasive Technology," B.J. Fogg clarifies how positive feedback and intermittent rewards help digital technologies to be deliberately shaped to change user behaviors. (Fogg 2003). In the context of cognitive warfare, these mechanisms are exploited to disseminate and reinforce manipulative messages, creating a feedback loop that can radicalize opinions and behaviors.

4. Impact of Cognitive Warfare on Society and Democracy

Cognitive war affects social cohesiveness, political polarization, and confidence in democratic institutions profoundly. Cognitive warfare players can destabilize whole societies by taking advantage of cognitive weaknesses and changing perceptions, so compromising the foundations of democracy and generating divisions among people. The great use of social networks and digital platforms in the setting already mentioned intensifies this phenomena.

Social cohesiveness is the link and feeling of belonging that ties together the people living in a society. Direct attacks on this cohesiveness by cognitive warfare include disinformation, propaganda, and false narratives encouraging divisions and hostility between many social groups. Cass Sunstein states "disinformation and propaganda can erode social cohesion by creating suspicion and hostility among social groups."(Sunstein 2014). One prominent example is the proliferation of pandemic-related conspiracy theories and false news, which have caused social fragmentation and raised tensions between many groups. These strategies of cognitive warfare have been destabilizing, so impairing societies' capacity for collective action and cooperation in the face of shared problems.

One other major result of cognitive warfare is **political polarization**. Cognitive warfare players can widen political divisions and radicalize public views by spreading false information and polarizing propaganda. This results in a more divisive political environment and difficulties arriving at consensus-based solutions. According to Nolan McCarty, political polarization "increases when people are constantly exposed to messages that reinforce their own beliefs and demonize the opposition."(McCarty, Poole and Rosenthal 2016). Cognitive warfare exploits social media algorithms that support content creation with the most interaction, so magnifying polarizing messages and further separating society.

The foundation of democracy is **trust in state institutions** Cognitive warfare often aims to undermine trust by disseminating false information and conspiracy theories challenging the legitimacy and efficiency of public institutions. Francis Fukuyama asserts that "trust in institutions is essential for social cohesion and the functioning of democracy." (Fukuyama 1996).

Direct effects on citizens' trust in democratic institutions are disinformation campaigns attacking the integrity of elections, the accuracy of the media, and the impartiality of the court system. These strategies might cause a general mistrust and cynicism, so undermining the basis of democracy and helping authoritarianism to grow.

Notable examples of cognitive war are the Brexit referendum and the 2016 U.S. presidential contest. In these instances, psychographic profiles created from the personal information of millions of Facebook users were used to target specific political ads during the specified referendum and election. Having a clear and obvious impact on society and the values of democracy, Carole Cadwalladr says "Cambridge Analytica used personal data to build detailed models of voter psychology and deliver personalized messages intended to manipulate electoral behavior" (Cadwalladr and Graham-Harrison 2018). Particularly ascribed to Russia, foreign intervention included disinformation and social media propaganda campaigns meant to polarize the American population and erode confidence in the voting system. The 2019 report of the former FBI director exposed that these initiatives used social media and created false narratives to influence voter opinions and spread divisive stories. (Mueller 2019). Regarding Brexit, false ideas about the effect of immigration and European Union membership were pushed forward using disinformation and propaganda campaigns. Social media and digital channels helped to magnify these messages, so fostering uncertainty and division among British people.

5. Defense and Resilience Measures Against Cognitive Warfare

Media education, digital literacy, and psychological resilience development all part of a multifarious and multilateral strategy needed to shield people and civilizations from the consequences of cognitive war. Using sensible policies and strategies will help to produce a society more informed, strong enough to resist cognitive manipulation.

To help people to recognize and evaluate the material they come across, **media education** is absolutely vital. This entails honing abilities to spot false information, grasp context, and evaluate information sources. Media education specialist Renee Hobbs underlines that "media education is not just about using technology, but about understanding how media influences society and developing critical thinking skills." (Hobbs 2011). Programs for media education can be included into adult continuing education courses as well as into school courses. These ought to comprise case studies, hands-on drills, and debates on how the media shapes society. Furthermore crucial for ensuring the relevance and timeliness of instructional resources as well as for offering different points of view is cooperation with journalists and communication experts.

Digital literacy is a crucial component of defense against cognitive warfare. It requires not only knowledge of digital technologies but also of how algorithms, social media platforms, and data collecting systems operate. Researching digital literacy, Helen Haste notes that "in the digital age, literacy must also include the ability to navigate and understand the complexity of digital environments." (Haste 2009). All age groups should be able to access digital literacy initiatives, which should comprise courses on online security, personal data protection, and acknowledgement of algorithmic manipulation. Governments, non-governmental groups, and technology companies can all help these projects guarantee sufficient resources and wide coverage.

Psychological resilience is a person's capacity for stress management and adaption to adversity. Developing psychological resilience can enable people in the framework of cognitive warfare resist manipulation and preserve critical thinking ability. According to George A. Bonanno "resilience is not a fixed trait, but a set of behaviors and skills that can be developed and strengthened" (Bonanno 2004). Stress management strategies, emotional intelligence development, and a growth mindset encouragement should all be part of programs aiming at psychological resilience. Building supportive communities where people may share and talk about experiences helps to improve social cohesiveness and lower isolation by means of which individuals might be more involved.

Policies and regulations. Developing laws and rules to protect societies against the effects of cognitive warfare falls mostly on governments and international agencies. These could cover rules about data protection, algorithm transparency, and digital platform accountability for the content they carry. One such a clear example is the European Union's General Data Protection Regulation (GDPR), which lays strict rules on the acquisition and use of personal data. The European Commission says "GDPR gives citizens more control over their data and imposes clear obligations on companies that manage personal data"**.** (European Commission 2018). Furthermore encouraged should be digital channels for creating and using defenses against manipulation and false information. Working with independent journalism organizations, enhancing fact-checking systems, and creating tools to let consumers report and fight misleading or manipulative content could all help to accomplish this.

Public awareness campaigns are crucial to inform people on the dangers of cognitive warfare and to advance a critical thinking culture. To properly reach a big and varied audience, these campaigns can use a wide spectrum of communication channels including traditional media, social networks, and community events. Organizations such as First Draft News and the Digital Forensic Research Lab are working to provide resources and training in recognizing and combating misinformation. Educating the public about misinformation techniques and how to recognize and combat them is crucial to maintaining an informed and resilient society.

International collaboration. Cognitive warfare is a global problem that requires international collaboration to address effectively. Working together, states and international organizations can create shared strategies, exchange data, and coordinate reactions to disinformation and manipulation campaigns. Initiatives like NATO's Working Group on Cognitive Warfare draw attention to how crucial worldwide cooperation is in creating sensible defense plans. (Allied Command Transformation 2023)

CONCLUSION

Different from informational and psychological warfare, **cognitive warfare** is a sophisticated development of non-kinetic conflict emphasizing subtle and deep manipulation of cognitive and emotional processes. Cognitive warfare becomes a potent weapon for influencing behavior and perceptions by means of advanced technologies and cognitive science insights, so posing new challenges and opportunities in military security and strategy. Its instruments are propaganda, contrived narratives, behavioural psychology, and the use of personal data to over time shape opinions and actions. Social media and digital channels magnify these effects by letting manipulative messages travel quickly and personally. Deeply affecting society and democracy, the effects compromise social cohesiveness, polarize politics, and erode confidence in democratic institutions. Deep knowledge of the mechanisms of cognitive warfare and the creation of resilience and defense strategies including media education, digital literacy, and international cooperation are absolutely vital if we are to safeguard democracies

BIBLIOGRAPHY

1. Allied Command Transformation. 2023. *NATO ACT.* April 05. Accessed June 02, 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.
2. Bonanno, G. A., 2004. "Loss, trauma, and human resilience: have we underestimated the human capacity to thrive after extremely aversive events?" 20. American psychologist 59, no. 1.
3. Bradshaw, S., and Howard, P. N., 2019. *philhoward.org.* Accessed 02 06, 2024. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf.
4. Cadwalladr, C., and Graham-Harrison, E., 2018. *The Guardian.* martie 17. Accessed 06 02, 2024. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
5. Ellul, J., 1965. "Propaganda: The Formation of Men's Attitudes". United States: Vintage Books.
6. European Commission. 2018. *European Union.* 05 23. Accessed 06 02, 2024. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.
7. Fogg, B.J., 2003. "Persuasive Technology: Using Computers to Change What We Think and Do". 283. Morgan Kaufmann.
8. Fukuyama, F., 1996. "Trust. The Social Virtues and the Creation of Prosperity". 480. United Kingdom: Free Press.
9. Haste, H., 2009. "What is «competence» and how should education incorporate new technology's tools to generate «competent civic agents»". 207-223. The curriculum journal 20, no. 3.
10. Hobbs, R., 2011. "Digital and Media Literacy, Connecting Culture and Classroom". 214. United Kingdom: SAGE Publications.
11. Libicki, M. C., 1995. "What is information warfare?" Strategic Forum Number 28.
12. Linebarger, P. M. A., 2015. "Psychological Warfare". United States: Hauraki Publishing.
13. London, J. H. University&Imperial College. 2021. *NATO.* May 20. Accessed June 02, 2024. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.
14. McCarty, N., Keith T. P., and Howard R., 2016. "Polarized America, Second Edition, The Dance of Ideology and Unequal Riches". 272. London: MIT Press Cambridge.
15. Mueller, R. S., 2019. "The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election". 445. e-artnow, ebook.
16. Nye, J. S., 2009. "Soft Power: The Means to Success in World Politics". United Kingdom: Public Affairs.
17. Singer, P. W., and Emerson T. B., 2018. "Likewar: The Weaponization of Social Media". United Kingdom: Houghton Mifflin Harcourt.
18. Sunstein, C. R., 2014. "On Rumors, How Falsehoods Spread, Why We Believe Them, and What Can Be Done". 109. United Kingdom: Princeton University Press.
19. Thaler, R. H., and Cass R. S., 2008. "Nudge. Improving Decisions about Health, Wealth and Happiness". United States: Yale University Press.
20. Waltzman, R., 2017. "The Weaponization of Information: The Need for Cognitive Security". 8. Rand Corporation.
21. Zuboff, S., 2019. "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019". United Kingdom: Profile.