Journal of Strategic Security

Volume 16 | Number 1 Article 3

Modern Cognitive Operations and Hybrid Warfare

Yuriy Danyk
y.danik@gmail.com

Chad M. Briggs
The Johns Hopkins University, cbriggs9@jh.edu

pp. 35-50

Recommended Citation
Danyk, Yuriy and Briggs, Chad M.. "Modern Cognitive Operations and Hybrid Warfare." *Journal of Strategic Security* 16, no. 1 (2023) : 35-50.
DOI: https://doi.org/10.5038/1944-0472.16.1.2032
Available at: https://digitalcommons.usf.edu/jss/vol16/iss1/3

Modern Cognitive Operations and Hybrid Warfare

Abstract

Concepts of cognitive warfare and operations are explored in the context of hybrid warfare, including how cyber technologies promote greater asymmetric opportunities for influence, control, and undermining of one's adversary. Research areas are analyzed in the interconnection with hybrid cognitive operations. The purpose of the article is to study the features and theoretical and applied substantiation of cognitive actions in cyberspace and through cyberspace and their possible consequences within the framework of hybrid conflicts.

Introduction

During the decades since the Cold War, world geopolitics have been marked by forms of turbulence, significant transformations, and growing contradictions. While national and international security have always been hybridized, at least partly, as state structures intertwine with non-state and economic actors, the scope of the security field has increased significantly. One major cause of the expansion of security risks can be attributed to the creation and development of cyberspace, including the control of mass dissemination of information, and increasing opportunities of influencing critical infrastructure and elements of organizational and technical systems. Certain states and non-state actors are attempting to leverage cyber and information technologies to control the actions of adversaries (and perhaps even allies).[1] The most effective actions are in the cognitive sphere, shifting the nature of available information and perceptions for targeted audiences.

Adversaries' efforts at cognitive control have complex impacts on both individuals and society, which malign actors can use to expand the sphere of domination and the transformation of an independent country into a neo-colonial relationship with another entity. Tools of information perception and manipulation can be used to achieve various political, economic, military, and other goals, which in some interpretations is a form of preventive defense.[2] If it is possible to weaken one's adversary or convince them that only certain alternatives are available, then conventional conflict can be avoided entirely.[3] Internet technologies allow for asymmetric leverage of such tools, with smaller state and nonstate actors now able to influence much larger entities at modest cost, at great distance, and often anonymously.

Given the high costs paid by aggressor states in kinetic warfare, often campaigns are carried out as hybrid conflicts, defined as actions carried out using a broad spectrum of tools to weaken or undermine one's adversary. Whether developed under the rubrics of 'unrestricted warfare' or maskirovka, hybrid conflicts often take advantage of Western notions and laws dividing war and peace, military, and civilians.[4] In a hybrid conflict where cognitive tools are employed, everyone is a target, even if notionally the country is at peace.

Cognitive Operations and Hybrid Cognitive Control

Modern hybrid conflicts and their influence on the highest level of human thought and values, form the basis for concern over future security trajectories. The battlefield in such wars is the territory of the human brain. In this article we highlight cognitive operations phenomena as the coordinated goal (target), scope, location, and time parallel and/or consequent actions, which support influence on the highest level of human thought, outlook, values, knowledge, and interests. Cognitive operations affect people's perception of reality and decision-making, guiding groups of people and targeted audiences towards conditions desired by a geopolitical adversary.[5]

Cognitive operations can also be effective tools for preventative actions to decrease the risks and threats of conventional wars. At the same time, cognitive operations can be tools of expansion or even specific colonization through transformations of outlook, values, and interests of targeted groups. Authors define hybrid cognitive control or expansion as a process of directed and controlled influence on system of values, outlook, knowledge, mental space, personal and social consciousness.[6] Such control can give new opportunities for state colonization in the digital era. Hybrid cognitive influences may appear during communication at different levels and of different natures. Cognitive operations can include specific socio-cultural and linguistic parameters. Influence or expansion efforts do not arise in a vacuum, but are deliberate and clearly directed processes, and not spontaneous and self-regulating. Operations occur through deep knowledge of the mental space of certain target groups and societies, and an understanding of how social and mental vulnerabilities.[7] Each of its components necessarily has its own customer, developer, and organizer.

Digital colonization can be treated as one of innovative and the most effective mechanisms in the digital era due to the influence on people and society using modern information technologies and artificial intelligence tools, carried out in and through cyberspace. Cognitive operations are aimed at managing the worldviews, interests, and values of people, unlike the seizure and colonization of a territory or economy of the state. That is, if in the past colonization involved the physical seizure of territories and economic systems, then in the modern world both can be controlled by transforming the cognitive sphere of the target groups through the use of

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

digital technologies. Digital colonization can also refer to data harvesting and influence efforts, such as where "tech companies extract, analyze, and own user data for profit and market influence with nominal benefit to the data source."[8]

As a result, we analyze the concept of wars of the future, as wars for the outlook, mind, feelings, and perception of people. Again, there is no clear distinction between hostile operations carried out by a nation state against another, or influence operations such as microtargeted carried out against select individuals by a tech company. At times such efforts can go together.[9]

We examine the relevant research concerned with different aspects of hybrid conflicts and cognitive actions. Most important, we emphasize cognitive warfare in terms of directions, levels of interconnectedness and spheres within which actions occur. Four categories where cognitive operations take place include:

- Physical influence zones, including infrastructure and information systems;
- Information and cyber space, where the information is created, processed, is being saved and spread;
- Cognitive processes, transformation of outlook, conscious, beliefs, interests, and values;
- Critical consequences of cognitive operations.

These categories are based upon research literature of cognitive warfare, but also direct experiences in the field of cyberwarfare in Ukraine and the neighboring region.

Analysis of the Research: Modern Hybrid Cognitive Operations as a Basic Component of Hybrid Conflicts

In the 21st century, there is no debate over the existence of hybrid conflicts, merely debates over definitions and the way national security institutions should respond. Such hybrid conflicts occur over the world. The military theorist Carl von Clausewitz described war as a "chameleon" that adapts to its environment.[10] In this sense, hybrid conflicts and wars are becoming a form of adaptation to the changes taking place in the world

of society and technology. These technologies provide opportunities for actors to take control and even in some way colonize entire states without occupation or visible use of the armed forces. An increasing number of modern conflicts fall into the category of "hybrid" and according to various experts, they may be the dominant form of conflict in this century.

The terms hybrid conflict, hybrid threats, and hybrid actions appeared in studies by experts from leading NATO countries in the late 1990s. One such author on the concept of hybrid warfare, Frank Hoffman, defined as "a full range of different modes of warfare including conventional capabilities, regular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[11] Elements unique to hybrid warfare and their application throughout history are described by Murray and Mansoor's monograph, as well as Russian and Ukrainian sources.[12] Gorbulin argues that although some elements of hybrid warfare are not new and were used in wars of the past, the consistency of these elements are unique in the modern world, as well as their application in the growing importance of information.[13]

Subsequent studies have examined the phenomena, forms, methods, and techniques concerning the origin, development and management of hybrid conflicts and technologies. Yet even before the concept of hybrid warfare, the scientific community recognized the transformation of international relations and the influences systematically organize cognitive influences. Basil Liddell-Garth in his book "Strategy of Indirect Action", first published in 1929, wrote that the goal is to disrupt the stability of the enemy, which may result in the collapse of an enemy army or ensure its defeat in combat.[14] One of the strategies that best suits the nature of hybrid warfare and its goals is the strategy of controlled chaos. Its task is to discredit the state, and impose notions of its unsustainability or illegality of its existence.

According to Filippovich, once incredible science fiction futures may soon come to pass. He includes nano-, bio-, info- and cognitive technologies in the areas of advanced technologies. Cognitive technologies play an equivalent and, eventually, a dominant role in this quartet.[15] J. Lewis's famous report deals with the use of a wide range of media, including television, the press, cinema and the Internet.[16] This helps to popularize any necessary narrative and promote the imposed point of view, not as a

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

simple “vote for X” formulation but rather a shift in identities, feelings of belonging, and worldviews. Libicki's views on the erosion of military and diplomatic norms, as well as how cognitive operations in hybrid warfare impede the separation of military and civilian spheres explain, in some sense, why some actors may choose hybrid conflict over kinetic warfare. [17] Pozeptsov believes that cognitive warfare operates at a strategic level, trying to destroy and divide target societies in peacetime through non-kinetic means. At the operational level, the strategy of cognitive warfare relies on information operations, the collection and dissemination of disinformation, propaganda, and politically sensitive information, both fake and real.[18]

Research Priorities and Results: The War of the Future for Outlook, Mind, Feelings and Perception

Four main areas should be focused on with respect to cognitive warfare and operations. The first are physical areas of impacts, including infrastructure and information systems. This is the more traditional domain of cyber operations and is a crucial component of cognitive efforts when used in synergistic ways. Local examples have included the Russian attacks on the Prykarpattyaoblenergo power station in Ukraine in late 2015, part of a larger, coordinated effort to undermine trust in Ukrainian state utilities.[19] Physical impacts can be larger in scope, such as attempts to redefine borders and resource access in the South China Sea.[20]

The second area of focus should be the information and cyber realms, where information is created, transformed, saved, and spread. Research here can include the influence of and by media and social media companies, mis- and disinformation campaigns, outside election interference, and even attacks against scientific data and research. Analyses of information during the COVID-19 pandemic, for example, focus not only on what information was available to people concerning the virus, vaccines, and public health status, but any intentional campaigns to undermine trust in vaccines, masks, or propagation of various conspiracy theories. It ultimately led to more COVID infections[21]and mass transfer to e-learning, which is becoming crucial on a global level.

The third area of focus are the cognitive processes themselves, meaning the worldviews, perceptions, awareness, beliefs, interests, and values.

Research on the psychological impacts of cyber interactions go back to Sherry Turkle in the 1980s, but there remains a need to understand and protect against various types and modes of influence.[22] How are teenagers affected by sharing visual information of peers versus text-based information, and how is this leveraged by outside actors?[23] How much are non-rational (limbic) systems affecting politics, and how are these being exploited?

Last, there are direct social/psychological impacts of cognitive operations. How have resilience targeting campaigns affected the outcome of larger conflicts, and where have they succeeded and failed? One of the most poignant examples here is of Ukraine, where concerted cognitive campaigns were carried out (and never exclusively by the Russian government) from 2014-2022, affecting much or most of Ukraine's prewar population of 44 million people. Before the events of 2022, when the conflict was more limited to eastern oblasts, researchers were surprised to discover that physical symptoms of trauma were being exhibited across the country, not only among the front-line populations.[24] The collective impacts of the hybrid-cognitive war across the country, including uncertainty over critical services, amplified allegations of corruption, fears over the continued conflict, and not knowing if they could rely upon the West for assistance.

What is notable in the Ukraine case was how such efforts to undermine Ukrainian resilience and morale were ultimately unsuccessful. Despite Russian government assumptions that a quick military operation into Kyiv would collapse the government and defense forces within 72-96 hours, the morale and resolve of people in Ukraine has been remarkably solid.[25] While one can point to various factors involved, including leadership of President Zelensky, swift support by allied government such as the United States, and various failures by the Russian military, the refusal of Ukrainian citizens to support or cooperate with Russian forces has been critically important for the course of the invasion.

Modern cognitive warfare is not a war in the literal sense of the word. It is not a conquest of geographical territory, but rather competition for the human mind and the ability to transform the worldview of people in society in a particular area. These cognitive maps are the territory for conquest in the framework of hybrid cognitive warfare, the information

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

battle space where perception of reality can be altered or constructed.[26] While information operations are hardly new, technologies allow for largely asymmetric actions, and the spread of information can both be largely beyond the ability of states to control, and the speed of dissemination (or virality) has grown exponentially.[27]

Western military science distinguishes four generations of warfare. The first three generations are those of classic war, with the use of force, military equipment, and physical logistics. The idea of fourth-generation wars originated during the Cold War.[28] During the struggle for presence in different parts of the world, superpowers realized the large-scale use of tanks, aircraft and missiles may be largely ineffective, and that the role of guerrillas in various political, economic, financial, information and psychological subversive operations increased dramatically. While the concept of irregular warfare was again hardly a new development, it ran counter to conventional military doctrines, as well as against laws and tradecraft of many countries in their foreign policies.[29]

While many information campaigns in past wars have focused on crucial aspects such as morale, the scope and intentions of modern cognitive-hybrid operations have both expanded and shifted. Destructive actions can combine various disinformation campaigns with cyberattacks on information resources, infrastructure, economic processes, and democratic institutions.[30] Cognitive operations therefore not only inject information into cyberspace, but are often coordinated with undermining the reliability and trust in critical systems and institutions such as state management, state security, social sphere, banks, hospitals, educational and scientific institutions and official sources of information. The intentions here are twofold: Redirect people away from traditional information sources, to undermine trust in official state institutions and the ability of a community to adequate respond to shifting outside conditions, attacks, or disasters.

By undermining trust in traditional information sources, it is possible to redirect people onto new media sites, including those heavily controlled or influenced by the aggressor. The conventional wartime use of radio stations such as Tokyo Rose relied upon scarcity of information along the front lines. Now people are flooded with information, but this can be curated or micro-targeted to specific populations via social media.[31] If

metadata are available indicating, for example, that particular users react to or discuss the topic of immigration frequently, news stories or disinformation can be directed toward them as a way of confirming their fears.[32] Many Western analyses of such tactics, such as the virtual societal warfare described by the RAND Corp., tend to focus on cognitive rationalization and availability of information, particularly how this may affect decision-making and election outcomes.[33] Where people receive their news, and the impacts this can have on concepts such as agenda setting, issue salience, anchoring, and priming, are important for politics and can be measured using established methods in political psychology.[34]

At the same time, the risk of so-called cognitive distortion increases. The risks can be presented in the form of four categories:

- When there is a lot of information (Problem: An overabundance of information)
- When there is not enough meaning (Complexity of understanding)
- When we react quickly (The need for a quick response)
- When we remember and recollect (The ratio of remembered and forgotten).

The equally important but perhaps more ephemeral impact concerns the second intention of cognitive operations, that of undermining trust in institutions and the resilience of communities. The undermining of trust and resilience may be more emotive in nature, not reliant upon rationalizations but more basic fears related to the brain's limbic system.[35] Everyone has the personal experience of being able to rationalize why someone should be trustworthy, and yet not trusting that person based on emotions or hunches (the opposite can also be true). Effective cognitive operations can exploit people's emotions, drawing upon their fears, aspirations, loyalties, and perceptions of others as a way of creating psychological outgroups and limiting perceived courses of action, for example, we cannot call the police, we keep hearing how corrupt they are, and people of other nationalities, views, orientations are alien to us, the bearers of traditional values. Such information is more readily to receive, when it is combined with effective cyber operations, for example, initiating a discussion of these issues in social networks, in various forums, in the blogosphere, combining this with cyber actions that increase public

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

discontent and distrust of the authorities as shutting down electronic access to information resources or disabling electrical power systems.[36]

Modern warfare is a complex and multifaceted socio-political phenomenon of a hybrid nature. It uses a variety of forces and means in a complex manner. It is carried out in almost all spheres of life and activity of people and states. In his memoirs, the Minister of Industry of Germany (1943-1945) Albert Speer pointed out that it was enough for the Allies to bomb several factories producing bearings and the entire industry and military equipment would stop within a few months.[37] In a contemporary analogy, if electronic microchips and bearings imports to the Russian Federation stop due to economic sanctions, then in a few months the production of electronics for the military sphere and mechanical engineering may stop there. But if, due to appropriately changed beliefs, worldviews, attitudes, and emotions (modulated and transformed because of purposeful cognitive influences), the employees of these factories consciously begin to sabotage the work that contributes to the war, the same result can be achieved much more efficiently and effectively without the use of conventional weapons. An even more powerful effect occurs when cultivating and promoting false scientific views and theories- for example, denial of climate change or COVID-19. Then the state, its economy and science are hampered in their development for many years and even decades. Sometimes the result of such an effect is almost impossible to overcome at all. It will manifest itself in one way or another in the future. This was the case in the former Union of Soviet Socialist Republics, where cybernetics and genetics were declared as pseudo sciences, hampering biological and environmental sciences for decades.[38]

As combined operations, these can be characterized as resilience targeting or weaponization of vulnerabilities.[39] As closely related concepts, they grew out of concern over deliberate destruction of environmental systems, with resilience targeting focusing initially upon postwar reconstruction.[40] The central idea remains the same, however, in attempting to undermine resilience of the community and therefore weakening its ability to respond to shifting conditions. Resilience targeting can take many forms, from destruction of infrastructure to increased political polarization and corruption, but was based around the intention of preventing a community from rebuilding following a conflict. If, for example, many thousands of landmines were spread in agricultural fields in Bosnia, it might be more

accurate to describe this not as a combat operation but a deliberate attempt to prevent farming communities from returning to those fields after the war. The same processes can be found in cyber operations, where norms, beliefs and values are shifted to such an extent that, to paraphrase Thomas Wolfe, one can never go home again. Not only will physical infrastructure be targeted, as we are witnessing with energy supplies in Ukraine by fall 2022, but psychological landscapes are being heavily influenced as well, with the intention of permanently disjointing what had been functioning communities.[41]

In this sense, resilience can also be defined in psychological terms as the ability to withstand outside pressures, in contract to more biological concepts of "bouncing back."[42] Undermining psychological resilience of a community can be an effective tactic when it encourages paralysis of action, polarizes communities, and frames certain actions as hopeless. Appropriately prepared and disseminated information about this fact can be used to create panic and / or negative reaction (for example, "hunger is inevitable"), changing attitudes towards state power (for example, "they do not protect us and do not do what they should") and many other consequences. Its rapid and purposeful dissemination with the appropriate interpretation is also ensured in and through cyberspace. Their result will eventually be changed perceptions and attitudes to what is happening, which will certainly influence the decisions people make, for example, during elections.

Cognitive operations both amplify these physical operations but can also operate in their own space. People can be led to distrust their neighbors, even when there is no rational reason for doing so. The most effective campaigns mask their origins, leaving people to believe that the source of information comes from their peers and neighbors, those their community consider authorities, thus either establishing their trust in the veracity of the information, or blaming their neighbors for something that may have originated from far afield.[43] This is the basis of 'reflexive control' doctrines in some cases, framing alternatives and possibilities in ways that appear to be organic and of one's own decision. In the case of the Russian invasion of Ukraine, such operations outside of Ukraine aim to frame Ukraine or NATO as the actual aggressor, amplify risks of nuclear escalation, and frame mediated cease-fires (with the Russian federation maintaining control of invaded territory) as the only rational choice for Western

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

countries. Such framing is not only directed as foreign policy decision-makers, but is meant to influence social groups and elections at a time when energy and food prices (linked to the conflict) are threatening the well-being of families.[44]

Features and Methods of Implementation

The issues of destructive cognitive actions and hybrid cognitive operations are directly related to the processes of emission, processing, interpretation, transformation, and internalization of knowledge in managed communication. The operations are conducted from strategic to tactical levels, from general to targeted effects on society as a whole and its separate components and specific target audiences with integrated use of linguistic, figurative, hidden media effects, mental and other effects at different levels of cybersocial interaction. Close to the concept of "hybrid wars" is the concept of "new wars", developed by British researcher Mary Kaldor. Kaldor identified several categories of differences between "new" and "old" wars, namely the diversity of state and non-state actors instead of regular armed forces, state power instead of achieving geopolitical interests, seizure of territories through political means and establishing control over the population instead of military seizure of territories. Mary Kaldor also sees the reasons for such changes in globalization and technology development. Essentially, and despite legal and institutional assumptions to the contrary, there are fewer divides between military and civilian targets.[45]

Analysts at the RAND Corp. noted that achievement of certain goals, previously only thought attainable by military force, can instead replace the tools and methods of warfare in cyberspace. The essence of such actions is for multiple actors to penetrate and influence state and non-state structures, in order to minimize the effectiveness of one’s adversary.[46] In this conception, there is no (or limited) open confrontation, but the aggressor actively influences the object of interest at different levels and in different spheres of human life, gaining partial or complete control over target audiences. Much of this influence or control can take place without any authentic attribution, meaning the real actors can remain hidden while other outsiders can be blamed, or domestic groups (real or astroturfed).

Information and communication technologies and cyberspace provided opportunities for these efforts manipulating, controlling, and managing consciousness. The efforts included fabrication of facts, misinformation, propaganda to form views, attitudes, stable preferences, perceptions, the need to establish security, fears, panic, all of which are components as part of the Russian military invasion of Ukraine. Political actors have determined how to manipulate policy agendas, shape public opinion, and reshape social and political identities. While each component may be studied discreetly, full spectrum analyses to understand hybrid conflicts must include all factors in context, including and crucially intentions and goals.

Thus, the main channels of cognitive influence today are information via cyberspace and their national clusters. Through various groups and communities, electronic media, and other forms of communication, society's goals are subject to sufficiently regulated and controlled influence. It ultimately leads to changes in worldview, values, knowledge, perceptions, views, and opportunities for a new specific type of digital colonization. Hybrid cognitive expansion always has a specific goal, which is set by its beneficiaries, customers, and organizers. Its implementation requires significant resources and opportunities, as well as time. Today, cyberspace is extraterritorial, universal, and global. It is not yet tied (except in some countries) to specific geographical borders. In the presence of space broadband access, it is poorly controlled at the national level. Therefore, at the moment, cybertechnology is the most important tool for the formation of collective and individual consciousness and social values. Modern information and cyber technologies allow the implementation of hybrid action strategies to achieve the goals of excessive impact on individuals and society as a whole at a distance and without the possibility of evidence-based identification of the aggressor. It means it is almost impossible to clearly establish who the aggressor is and to prove guilt within the framework of the existing international law.

Conclusion and Prospects for Further Research

In examining cognitive operations, they are most easily understood in the context of hybrid warfare and large-scale attempts to undermine or weaken one’s adversary. The use of history, culture, worldview, religion, language, science, and education is of great importance, as these are the

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

main areas in which and through which hybrid cognitive influence is carried out and takes place. At times aggressors are content with sowing chaos and uncertainty, but several actors see cognitive operations as part of a larger strategic plan. Cognitive operations, as consciously controlled acts, are always based on specially developed strategic algorithms, which are adjusted depending on changes in the communicative context. Which narratives should be promoted, what forms of mis- or disinformation should be inserted into discussions, what fears or aspirations are being leveraged to achieve established goals?

More research is therefore needed into the field of cognitive operations to provide some early warning of its pathways and impacts. If such operations are detected, it is necessary to deploy system of counteraction and neutralization. Most of the processes involved in transforming the cognitive sphere are long-term, multifaceted, and well-thought-out actions, which cannot be easily counteracted after the fact. This includes identification of who the actors are. It is too easy to point fingers at the governments of the Russian Federation and People's Republic of China, while many malign actors are closely associated with criminal organizations, economic actors (including corporations), or mercenaries hired by well-funded organizations. Again, climate change provides a well-documented example of such processes, where concerted information campaigns were carried out by corporations in cooperation with certain petrostates in attempts to protect fossil fuel markets.[47] While such climate science debates were considered academic in many Western countries, for a government such as the Russian Federation protection of oil and gas export markets was (and remains) a central national security imperative.[48]

The practical value of such research can be to describe and identify a wide range of systemic and complex hybrid communication effects and interactions, allowing better early warning of such efforts by malign actors, and protection of social fabrics of trust, resilience, and healthy political discourse.

Endnotes

[1] Alexander Klimburg, "Mobilising Cyber Power." Survival 53, no. 1 (2011): 41-60, https://doi.org/10.1080/00396338.2011.555595.

[2] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* 5, no. 2 (2011): 95-112, https://www.jstor.org/stable/26270559.
[3] Blagovest Tashev, Michael Purcell, and Brian McLaughlin. Russia's Information Warfare: Exploring the Cognitive Dimension. Marine Corps University Journal 10, no. 2 (Fall 2019): 129-147, https://doi.org/10.21140/mcuj.2019100208.
[4] Gregory Commin and Eric Filio, "Unrestricted Warfare Versus Western Traditional Warfare: A Comparative Study." *Journal of Information Warfare* 14, no. 1 (2015): 14-23, https://www.jstor.org/stable/26487515.
[5] Margarita Levin Jaitner and Harry Kantola, "Applying Principles of Reflexive Control in Information and Cyber operations," *Journal of Information Warfare* 15, no. 4 (2016): 27-38, https://www.jstor.org/stable/26487549.
[6] Eve Hunter and Piret Pernik, The challenges of hybrid warfare. Tallinn: International Centre for Defence and Security, 2015: 4, https://icds.ee/wp-content/uploads/2013/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf.
[7] David Tayouri, "The Secret War of Cyber Influence Operations and How to Identify Them." Institute for National Security Studies Cyber, Intelligence, and Security Publication 4 (2020): 5-22, https://www.inss.org.il/wp-content/uploads/2020/03/Cyber4.1ENG_e-5-22.pdf
[8] Danielle Coleman, "Digital colonialism: The 21st Century Scramble for Africa Through the Extraction and Control of User Data and the Limitations of Data Protection Laws." *Michigan Journal of Race & Law* 24 (2018): 417, https://doi.org/10.36643/mjrl.24.2.digital.
[9] Hal Berghel, "Malice Domestic: The Cambridge Analytica Dystopia." *Computer* 51, no. 05 (2018): 84-89, https://doi.org/10.1109/mc.2018.2381135.
[10] Carl Von Clausewitz, *On War* (Princeton University Press, 2008), 30.
[11] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007), 8.
[12] Nathaniel D. Bastian, "Information Warfare and Its 18th and 19th Century Roots," *The Cyber Defense Review* 4, no. 2 (2019): 31-38, https://www.jstor.org/stable/26843890; Volodymyr Gorbulin, Vlasyuk Olexander, and Serhiy Kononenko, *Україна і Росія: дев'ятий вал чи китайська стіна* [Ukraine and Russia: The Ninth Wave of the Chinese Wall] (Kyiv: The National Institute of Strategic Studies, 2015); Williamson Murray and Peter R. Mansoor, eds. *Hybrid warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge University Press, 2012).
[13] Volodymyr Gorbulin, "Гібридна війна" як ключовий інструмент російської геостратегії реваншу," ["Hybrid War" as a Key Tool for Russian Geostrategic Revenge] *Стратегічні пріоритети* 4, no. 33 (2014): 5-12, http://www.library.univ.kiev.ua/ukr/elcat/new/detail.php3?doc_id=1617128.
[14] Basil Liddell Hart, "Strategy. The Indirect Approach." in *Strategic Studies*, edited by Thomas Mahnken, Joseph Maiolo, and Joseph A. Maiolo (London: Routledge, 2008), 101-104, https://doi.org/10.4324/9780203928462.
[15] Andrej Filippovich, "Инфо-когнитивные технологии в подготовке космонавтов" [Info-Cognitive Technologies in the Training of Cosmonauts]. Personal blog, September 4, 2012, http://blogs.it-claim.ru/andrey/2012/09/04/info-cognitive-technology-space/.
[16] James Andrew Lewis, *Cognitive Effect and State Conflict in Cyberspace* (Washington, DC: Center for Strategic and International Studies, 2018), https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace.
[17] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007).
[18] Georgii Pocheptsov, "Cognitive Attacks in Russian Hybrid Warfare," *Information & Security* 41 (2018): 37-43, https://doi.org/10.11610/isij.4103
[19] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* 9 (2016): 1-10, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032

[20] Ketian Zhang, "Cautious Bully: Reputation, Resolve, and Beijing's Use of Coercion in the South China Sea," *International Security* 44, no. 1 (2019): 117-159, https://doi.org/10.1162/isec_a_00354.
[21] Simon Springer and Vural Özdemir, "Disinformation as COVID-19's Twin Pandemic: False Equivalences, Entrenched Epistemologies, and Causes-of-Causes," *OMICS: A Journal of Integrative Biology* (February 2022): 82-87, https://doi.org/10.1089/omi.2021.0220
[22] Sherry Turkle, *Life on the Screen* (New York: Simon and Schuster, 2011).
[23] Giulia Ballarotto, Barbara Volpi, and Renata Tambelli, "Adolescent Attachment to Parents and Peers and the Use of Instagram: The Mediation Role of Psychopathological risk," *International Journal of Environmental Research and Public Health* 18, no. 8 (2021): 3965. https://doi.org/10.3390/ijerph18083965.
[24] Yuriy Danyk, O. Zborovska, and N. Rodina, "Models and Mechanisms of Formation of Posttraumatic Stress Disorders in Hybrid War Conflicts and Their Features," *Фундаментальні та прикладні дослідження у практиках провідних наукових шкіл* 31, no. 1 (2019): 44-53, https://doi.org/10.33531/farplss.2019.1.09.
[25] John Spencer and Lionel Beehner, "Why Morale is So Crucial in War." *Kyiv Post*, May 24, 2022, https://www.kyivpost.com/ukraine-politics/why-morale-is-so-crucial-in-war.html.
[26] Keith Scott, "'Nothing Up My Sleeve': Information Warfare and the Magical Mindset," in *Cyber Influence and Cognitive Threats*, edited by Vladlena Benson and John Mcalaney (London: Academic Press, 2020), 53-76, https://doi.org/10.1016/b978-0-12-819204-7.00004-x.
[27] Georgii Pocheptsov, *Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях* [Cognitive Wars in Social Media, Mass Culture and Mass Communications], (Oosterhout, Netherlands: Glagoslav Publications, 2019).
[28] Thomas X Hammes, "The Evolution of War: The Fourth Generation," *Marine Corps Gazette* (September 1994), https://newtotse.com/oldtotse/en/politics/us_military/162582.html.
[29] Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* 50, no. 3 (2006): 395-411, https://doi.org/10.1016/j.orbis.2006.04.002.
[30] Georgii Pocheptsov. "Cognitive Attacks in Russian Hybrid Warfare," *Information & Security* 41 (2018): 37-43, https://doi.org/10.11610/isij.4103.
[31] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017): 50-85.
[32] Sanne Kruikemeier, Minem Sezgin, and Sophie C. Boerman, "Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses," *Cyberpsychology, Behavior, and Social Networking* 19, no. 6 (2016): 367-372, https://doi.org/10.1089/cyber.2015.0652.
[33] Michael J. Mazarr, Ryan M. Bauer, Abigail Casey, Sarah A. Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica, CA: RAND Corporation, 2019), https://doi.org/10.7249/rr2714.
[34] Shanto Iyengar and Donald R. Kinder, *News That Matters: Television and American Opinion* (Chicago: University of Chicago Press, 2010).
[35] Linton Wells, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *Prism* 7, no. 2 (2017): 4-17, https://www.jstor.org/stable/26470514.
[36] Tamara Maliarchuk, Yuriy Danyk, and Chad M. Briggs, "Hybrid Warfare and Cyber Effects in Energy Infrastructure," *Connections* 18, no. 1/2 (2019): 93-110, https://doi.org/10.11610/connections.18.1-2.06.
[37] Albert Speer, *Inside the Third Reich* (New York: Simon and Schuster, 1997).
[38] David Joravsky, *The Lysenko Affair* (Chicago: University of Chicago Press, 2010).
[39] Kimberley Anh Thomas and Benjamin P. Warner, "Weaponizing Vulnerability to Climate Change," *Global Environmental Change* 57 (2019): 101928. https://doi.org/10.1016/j.gloenvcha.2019.101928.

[40] Chad M. Briggs, Moneeza Walji, and Lucy Anderson, "Environmental Health Risks and Vulnerability in Post-Conflict Regions," *Medicine Conflict and Survival* 25, no. 2 (2009): 122-133, https://doi.org/10.1080/13623690902943362.
[41] Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," *Survival* 64, no. 5 (2022): 7-26, https://doi.org/10.1080/00396338.2022.2126193.
[42] David Fletcher and Mustafa Sarkar, "Psychological Resilience: A Review and Critique of Definitions, Concepts, and Theory," *European Psychologist* 18, no. 1 (2013): 12, https://doi.org/10.1027/1016-9040/a000124.
[43] Samantha Bradshaw and Philip Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," Project on Computational Propaganda Working Paper (December 2017), https://demtech.oii.ox.ac.uk/research/posts/troops-trolls-and-troublemakers-a-global-inventory-of-organized-social-media-manipulation/. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no.1-2 (December 2014): 4-37, https://doi.org/10.1080/01402390.2014.977382.
[44] Olga R. Chiriac and Jahara Matisek, "Homeland Defense in the Information Space: Learning from Russian Influence Campaigns in Eastern Europe," Modern War Institute, October 19, 2022, https://mwi.usma.edu/homeland-defense-in-the-information-space-learning-from-russian-influence-campaigns-in-eastern-europe/; Ivana Stradner, "Russian Disinformation and Propaganda in Relation to the War Against Ukraine," Testimony to the Subcommittee on Security and Defence; Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation. European Parliament, May 17, 2022, https://www.fdd.org/analysis/2022/05/17/russian-disinformation-propaganda/.
[45] Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (New York: John Wiley & Sons, 2013).
[46] Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
[47] Naomi Oreskes and Erik M. Conway, "Defeating the Merchants of Doubt," *Nature* 465, no. 7299 (2010): 686-687, https://doi.org/10.1038/465686a.
[48] Chad M. Briggs, "Climate Change and Hybrid Warfare Strategies," *Journal of Strategic Security* 13, no. 4 (2020): 45-57, https://doi.org/10.5038/1944-0472.13.4.1864.

https://digitalcommons.usf.edu/jss/vol16/iss1/3
DOI: https://doi.org/10.5038/1944-0472.16.1.2032