

INFORMATION WARFARE IN THE CONTEXT OF MEDIA NETWORKS IN THE DIGITAL AGE

Nicoleta Annemarie MUNTEANU
“Lucian Blaga” University of Sibiu, Romania
nicoleta.munteanu@ulbsibiu.ro

ABSTRACT

The globalization of media communication has led to increasingly sophisticated methods, making the transmission of information at a fast pace that exceeds known range limits. One way that may arise and favorably perpetuate the information war is through media networks. By controlling the media, the manipulator can influence people, aiming to create a favorable attitude toward themselves. Our research examines the evolving relationship between technologies and media networks, exploring whether the convergence of digital technologies and media networks continue to fuel the persistence of information warfare as a strategic tool. We intend to present the interference of media networks and information warfare, the theoretical framing of the two concepts, but also folding these theoretic issues into practice, to demonstrate that media networks are a powerful factor influencing the information war. The research affirms that while technological advancements continue to reshape the nature of information warfare, media networks remain a central and potent tool in global power struggles, demanding heightened awareness and regulatory frameworks to address emerging challenges.

KEYWORDS: mass media; information warfare; mass communication; networks; informational environment

1. Introduction

The information age is characterized by the dominance of new types of wars, consisting of three different but interacting and interconnected realms of existence, the informational, physical and cognitive realms (Alberts et al., 2001, p. 320). Among these is being conquered by a warfare that bears its name and is driven by it – information warfare (IW) – a war for information, through information, and of counter-information. Among the wars of the supreme byte era, this is the most complex, the most modern, and the most formidable. The particularity of the IW lies in the global informational environment in which it operates; it is a type of war (Galeotti, 2022, pp. 160-165) that attacks the social environment through alteration

and influence, through the obsession with knowing, as well as through the proven tendency to prevent the adversary from knowing or to supply them with erroneous information through disinformation.

From the standpoint of conceptual delimitation, the notion of hybrid warfare continues to exhibit a series of inconsistencies, as no universally accepted definition currently exists – at least not within the framework of NATO’s taxonomy, where NATO is commonly regarded as a doctrinal point of reference (Ducaru, 2016, pp. 7-23). Within this context, certain scholars contend that hybrid warfare has effectively become a cat out of the box (Vincenzo, 2025, pp. 33-42), thereby complicating both theoretical and operational approaches to the concept. It is,

therefore, crucial to acknowledge the broader impacts and consequences of hybrid warfare, particularly regarding its influence on human rights and the emergence of cognitive warfare (Maslen, 2024, pp. 101-125). This latter dimension has already been conceptualized within the North Atlantic Treaty Organization through the framework of NATO COGWAR - NATO Cogwar Perception (NATO, 2025). Cognitive warfare should not be understood merely as an instrument of conflict, but rather as the very domain in which conflict unfolds. Within this paradigm, the human brain emerges simultaneously as the principal target and the primary weapon in the struggle for cognitive dominance. Engagement in this sphere entails the orchestration of deliberate, coordinated military and non-military actions, distributed across the entire spectrum of competition, with the explicit purpose of acquiring, sustaining, and safeguarding cognitive superiority (NATO, 2024). Conventional instruments of warfare – such as aircraft, bombs, and missiles – are increasingly being displaced by non-kinetic means, including cyberattacks, malicious software, and disinformation operations. Within the digital domain, adversaries possess the capability to probe and challenge security architectures through actions as minimal as a single keystroke (Munteanu, 2025, p. 209).

As a part of hybrid warfare, IW gets certain characteristics; especially considering the hybrid warfare as not being a new war, or the next phase of armed conflict, as Mumford and Carlucci state in one of their study, but “*rather an option at the disposal of great powers to achieve their political objectives in an era characterised by a high degree of competition and mistrust*” (Mumford & Pascal, 2023, pp. 192-206). Admitting this hypothesis, our analysis is focused on the connexions between the media effect on the informational environment, in terms of

vulnerabilities, threats and risks, and the IW. The complexity of this relation is under the umbrella of the ongoing technology that is about to increase the challenges of dealing with a continuous process of change. Information warfare (IW) represents a constitutive dimension of hybrid warfare, functioning through the integration of cyber operations, disinformation campaigns, and psychological influence mechanisms designed to erode adversarial stability in the absence of direct kinetic engagement. By systematically targeting cognitive processes, decision-making structures, and the resilience of societal cohesion, IW operates as a force-multiplier that enhances both conventional and irregular modalities of conflict, thereby intensifying the multidimensional efficacy of hybrid strategies across political, military, and civil domains (Fridman et al., 2019).

2. Methodology

This study adopts a qualitative research design, combining discourse analysis with network mapping to examine the nexus between information warfare and media networks. Primary materials include policy documents, strategic communication reports, and media content generated during recent geopolitical crises. Secondary sources encompass peer-reviewed literature on information operations, security studies, and digital media ecosystems. Methodologically, the research integrates content analysis to identify narratives and framing strategies, alongside social network analysis to trace dissemination patterns across traditional and digital platforms. This dual approach ensures both theoretical grounding and empirical validation of the enduring relevance of information warfare.

3. The Evolution of the IW in Contemporaneity

A series of elements make up the components of the IW, such as virtual,

psychological, electronic, hacker, economic, financial, cultural, and religious warfare. These elements can be characterized as the environments where the effects of informational warfare are most evident. In this context, the informational strategic war represents the intersection between the strategic warfare post-Cold War approaches and concepts and the IW evolution, as it is described in Figure no. 1. The informational strategic war requires special attention and recognition as a new and legitimate face of warfare, having implications related to the

national security strategy. The cyberspace characteristics have evolved increasingly lately and offer new opportunities for the IW by its emergency. From our point of view, it is important to understand all the elements and the interdependencies between them, as a precondition of an analytical approach related to the IW in its relationship with mass communication. Daily realities prove without any equivoque that cyberspace vulnerabilities will increasingly put pressure on strategic information warfare.

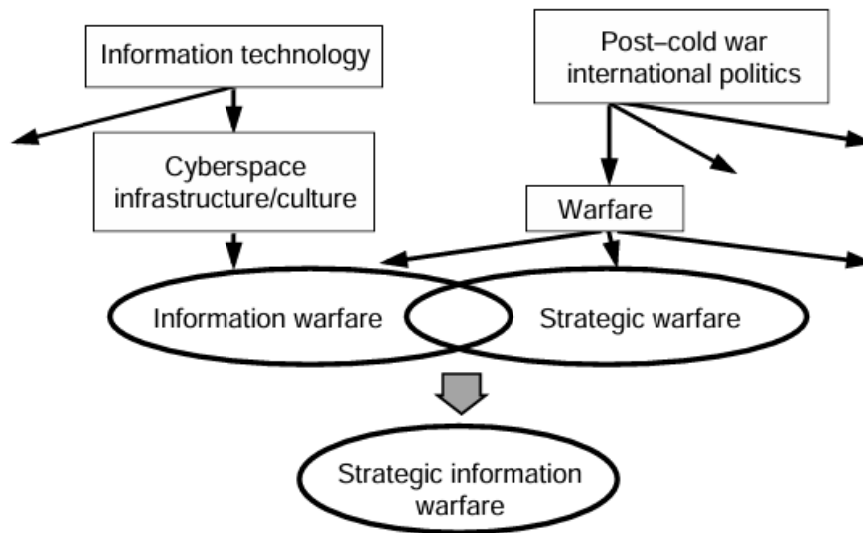


Figure no. 1: *Strategic Information Warfare*
(Source: Molander et al., 1996, p. 27)

The association of new warfare domains with information represents another revolution that requires specific capabilities and has significant effects on military organizations and operations. This concept refers to IW, or the struggle between two or more actors for control over the information battlefield, also known as the information space. While there is no universally accepted definition, IW can be broadly understood as any action intended to misinform, disrupt, degrade, or destroy an enemy's information and functional capabilities while simultaneously protecting one's own or allied forces against similar actions executed

by the adversary and ensuring the functionality of one's information systems (Topor, 2006, p. 21).

As a new form of strategic warfare, the IW is highly dependent on the vulnerabilities of socioeconomic systems. The primary question is how to attack the enemy's system while safeguarding one's own. However, information warfare itself, independent of other elements, represents a vulnerability for those who engage in it. This is because its use creates problems that extend beyond military structures and impact the entire security infrastructure. The societal environment characteristics

lead us to the link between warfare, as a general concept, and political warfare, cultural warfare (also approached in this context as cultural subversion) (Arquilla & Ronfeldt, 1997, pp. 23-24) or economic warfare. Another term continues to reach more approaches from the research field, being directly connected with the IW – media operation, considered as an important element in assuring the possibility to monitor and facilitate the understanding by the public opinion. Lately, this concept has become complementary to military operations (Munteanu, 2019, pp. 46-52), in terms of tactics, operations and strategy.

The concept of information warfare was first theorized in 1976 by Thomas P. Rona. The publication of Alvin Toffler's book *The Third Wave* (Toffler, 1983) in 1980 further laid the groundwork for this concept. Toffler suggested that to attack a nation, one could obstruct the flow of information, sever the connection between a multinational company's headquarters and its foreign branches, and erect informational barriers around it. This gave rise to a new term: "information sovereignty" which Toffler expanded upon in his later book *War and Anti-War* (Toffler, 1995). This concept has since been widely debated in the United States and beyond.

While the idea of IW, as it is understood today, has only been developed in recent decades, its fundamental principles can be traced back twenty-five centuries to the writings of the Chinese philosopher Sun Tzu. He emphasized deception as the key to warfare: "*All warfare is based on deception. Therefore, if you are capable, feign incapacity; if you are active, feign passivity. If you are near, make it seem as if you are far away, and if you are far, make it seem as if you are near. Lure the enemy into a trap; simulate disorder and strike*" (Sun, 2004, p. 10). Some of these ideas were later echoed by Machiavelli in the 15th century in *The Prince* and *The Art of War*, where he

stressed that a statesman must, above all, be a military leader with a calculated and cunning nature.

To better understand the essence of IW, we turn to Martin Libicki's (1995, pp. 123-126) classification, which categorizes IW based on attack-defense strategies and the types of information weapons used. According to Libicki, there are seven forms of information warfare. Command and Control Warfare refers to a strictly military form of information warfare aimed at disrupting an adversary's command and control systems through psychological operations, operational security, deception, electronic warfare, and physical destruction; Intelligence-based warfare involves designing, protecting, and dismantling systems that contain the necessary knowledge to dominate a conflict space; Electronic Warfare uses electronic technology and cryptographic techniques to control the electromagnetic spectrum; Psychological Warfare utilizes information to shape the attitudes and choices of allies, neutral parties, and adversaries; Hacker Warfare involves cyberattacks using malicious software against information systems; Economic Information Warfare aims to block or manipulate information to create a distorted image and gain economic supremacy; Virtual Reality Warfare uses the internet as a propaganda tool in a global information battlefield. Although this classification has been debated and expanded upon, it provides a useful framework for understanding the interdependencies between information warfare and media networks. This is the most used typology in the 1990^s and the beginning of 2000^s, by many scholars, but continues to stand out as one of the most well and widely developed and cited works (Wolterman, 2019, p. 10).

In recent years, there has been increasing attention from politicians, strategists, scientists, and the media regarding the theory and practice of

information warfare. This is particularly evident in North America and Europe, where public speeches, conferences, symposiums, books, studies, and articles frequently address the topic. The mass media, which primarily serves to inform, has also shifted its focus toward analysing information warfare, producing content aimed at a specialized audience. This highlights mass media's second major function: shaping public opinion and reinforcing its growing role in the realm of information warfare.

For millennia, the goal of war has been to destroy the enemy's forces and force them to negotiate on previously unacceptable terms. While this objective remains unchanged, the methods and means of warfare continue to evolve. Information has become one such method, leading to a new form of warfare in which battles may be fought and won without the adversary even realizing they were targeted (Zeca, 2002, p. 44). The growing importance of winning the information war is now a fundamental principle in modern conflicts.

Ultimately, IW can be viewed as a form of total war that incorporates multiple dimensions – electronic, psychological, imagery-based, and even parapsychological – alongside operations involving intelligence gathering, misinformation, jamming, surveillance, subversion, reconnaissance, obstruction, and disorganization. These elements form a pattern of escalation, progressing from aggressive actions and crises to full-scale conflicts and war. This progression aligns with Clausewitz's assertion that warfare cannot operate by its laws alone but must be understood as part of a broader political framework (Clausewitz, 1982, p. 612). Related to this assumption, Kuel is questioning whether IW can truly be considered war in the traditional Clausewitzian paradigm of violence and force (Kuehl, 2002, pp. 49-52).

The understanding of the modern IW could be accomplished only within the interconnections between the two dominant geopolitical spheres that have shaped the world since the Cold War – the Western one and the Eastern one (Wrobel, 2022, p. 58). Another aspect that contributes to a better understanding, even in terms of effect, is the existence of new threats in the informational environment, directly related to technology and the cybersphere.

4. The Interdependencies between IW and Media Networks

In our attempt to characterize the media impact, we start by presenting the communication process within mass communication. Mass communication involves the presence of specific elements with distinct functions (Fiske, 2003, p. 23): the source transforms information into a message by selecting signs and symbols and encoding them; the transmitter converts the message into signals, making it transmittable, such as electrical impulses; the channel ensures the transport of information or signals through air, cable, or wire; the receiver transforms the signal back into a message; the recipient deciphers the message and interprets its meaning. We also want to highlight a crucial component directly related to the interference between the media network and information warfare: communication jamming, which reduces transmission and decoding efficiency.

The interdependence between media and IW is also based on the information environment as presented in Figure no. 2. The synchronicity between the physical dimensions, information and cognitive represents the base for an effective IW, as a part of the hybrid war. Each element represents a tool to be studied and to conduct to the idea that media is in concordance with all, so that it could be considered a weapon, not just a means of conveying information (Mais, 2023, p. 60).

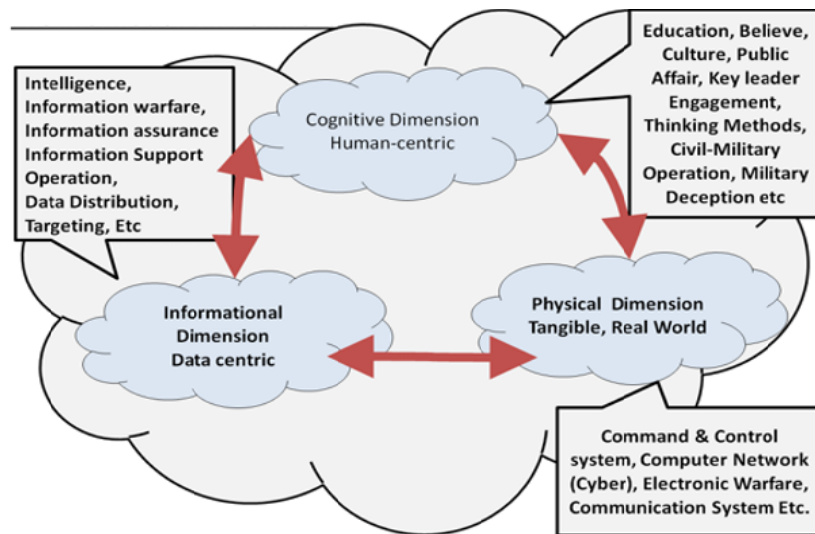


Figure no. 2: *The Information Environment*
(Source: Bakshi, 2018, p. 183)

Another main interdependence between the IW and media networks lies in the conveying the information into media, which enables the disappearance of borders, the overcoming of linguistic barriers, the reduction of cultural obstacles, and even the resolution of social crises triggered between elites and the common world. Another important aspect in terms of the strategic implications and outcomes is directly related to information and communication technology (ICT) (Wolterman, 2019, p. 10), given the characteristics of the current and the future political warfare and conflict.

The communicational effects in this fast-paced century are largely due to the existence of mass communication through media networks; these effects are more than evident in the military sphere, as in any other domain, since information acts everywhere, and mass communication channels facilitate its dissemination. The multiplication, diversification, and massive expansion of mass communication means, along with technical support systems, from traditional mass media such as print and audiovisual press to new communication media based on the convergence of telecommunications, informatics, and television, constitute the logistical

foundation of media networks (Libicki, 1995, pp. 123-126). The convergence of telecommunications, informatics, and television serves as the premise for a mediated communication system, a media network that merges the two primary forms of mediated communication: one that facilitates information exchange between individuals and another that is strictly mass communication, aimed at a collective audience (Drăgan, 2007, p. 286).

When discussing the concept of a media network, we also refer to the notion of the market in analyzing the media landscape. Media entities function as enterprises, “cultural industries” (Lochart & Bozer, 1998, p. 43), subject to market dynamics and competition, leading to restructuring movements, alliances, the formation of press groups, and multinational media corporations – so-called media networks. These include newspapers, publishing houses, television stations, and internet access providers. The increasing industrialization of this sector translates into a merchandising phenomenon of mediated communication, indicating a growing subjection to market-driven commercial logic.

From the perspective of information warfare, media is particularly relevant due to its cultural impact, as it revisits older theories of mass society through new interpretative frameworks applied to media culture. This aspect is crucial because mass communication directly affects the recipients of the message, the audience, which is a delicate matter since the audience belongs to two different spheres: civilian and military, each with its specific characteristics. The actors in mass communication, both transmitters and receivers, are more often collectives than individuals, and their behaviour has a collective nature. Thus, mass communication is complex and operates on a large scale by bringing together organized groups of message producers with private audiences who, although they may not perceive themselves as such, function as collectives. The mass media are intended for large-scale reproduction and communication with a mass audience (McQuail, 1999, pp. 173-174).

Introduced in the 1960^s by Marshall McLuhan (Marshall McLuhan, 1911-1980, was a Canadian philosopher, regarded as one of the main theorists and practitioners of the media industry, known for the expressions “the medium is the message” and „global village”), the expression “global village” suggests an extensive exchange of information and global knowledge transfer (McLuhan, 1997). In recent years, this level of communication has seen spectacular growth. Here, the transmitter addresses everyone indiscriminately through a channel to which any receiving entity has unconditional access, at least to the extent that access depends on the transmitter. Across all fields - military, cultural, political, and economic – the increasing dependence on mass media is evident, as information has become an increasingly globalized market where traditional borders are becoming less relevant.

The essence of IW – an attack on IT-based communication systems – requires

specific management of information, knowledge, communication, relationships, and responses to information manipulation, as well as human behaviour modification, practices employed by adversaries. Information, the true commodity, is transmitted, received, restricted, or stolen in secrecy; information manipulators are, in fact, manipulators of human consciousness in a war that represents the military manifestation of the information society, known as the third wave (Toffler, 1983).

Media visibility, facilitated by media networks, represents both an asset and a risk for an entity’s image, credibility, and legitimacy. A new and distinct type of vulnerability emerges (Thompson, 2000, p. 136), composed of four categories of elements generated by media visibility, including information leaks. This is particularly relevant to our discussion since the suppression or concealment of certain information can be interpreted by the media in various ways. The press considers it a duty to ensure public access to information held by the military, if national security interests are not compromised. However, in many cases, classified information hides potentially compromising details. The media plays a crucial role in exposing those who manipulate, hide, or release information, but it also tends to exaggerate and manipulate information itself. For this reason, media activities should maintain the highest possible level of objectivity, just as those working in this field should strive to do.

Freedom, in general, and press freedom, in particular, can be tempting for some to exceed the proper limits of journalistic practice. Sometimes, press freedom is perceived as the right to write anything about anyone, leading to the publication of immoral content, including pornography, or articles and commentaries that smear individuals unscrupulously using indecent or vulgar language (Turianu & Doru, 1996, p. 14).

There is much debate about the limits of journalism – the boundaries of information collection, the values upheld by those controlling the media, editorial culture, and audience preferences. However, we believe the most viable limits are those imposed by journalists themselves. If a journalist strives for professionalism, the risks that may arise will not be seen as temptations. The aspiration for professionalism, combined with a clear conscience, are two essential elements in defining a good journalist (Munteanu, 2009, p. 137). We take this perspective to emphasize that objectivity is the key element in defining a professional media network – one that demonstrates accuracy in its content presentation.

5. Media as a Vulnerability within the IW

Societal dependence on information is evident; information clarifies, evaluates, shapes, or transforms the situation and meaning within the physical operational context, referring to the aerial, maritime, terrestrial, and electromagnetic environments. It also applies to the human context (populations, groups, ethnicities) and the structural context (political, administrative, economic, military, cultural). Understanding and monitoring the media within a habitual environment is a key aspect of preventive communication management.

In this regard, mass communication through media networks supports our approach: information permeates all the previously mentioned environments, addresses a heterogeneous audience, and is not only accessible but also desired. Therefore, controlling media networks, thus controlling information, automatically leads to superiority for those who possess this control. Even more so, the information era that influences information warfare in all its forms is largely due to the existence of media networks. Information itself can

become an environment, known as the infosphere (Rotaru, 2003, p. 170). We are witnessing a war of crises, where the strategic evolution of the informational environment turns into a broad-front offensive, with specific targets and effects.

Similar to the discourse surrounding the so-called “CNN effect” in the 1990^s, contemporary analyses often rest on the presupposition that government decision-makers initially occupy the role of consumers of real-time media content before transitioning into agents who shape the information environment through policy interventions. Taken together, the characteristics of digitally networked yet highly fragmented public spheres, and the corresponding volatility in where discursive authority is situated, underscore the need to transcend conventional, state-centred analytical frameworks. Taken together, the characteristics of digitally networked yet highly fragmented public spheres, and the corresponding volatility in where discursive authority is situated, underscore the need to transcend conventional, state-centred analytical frameworks (Gilboa, et al., 2016, pp. 661-662).

The increasingly lower cost of accessing media networks, digitalization that facilitates manipulation and forgery, and the mobility of communication tools – mobile phones, satellite connections, and the internet – allow mass communication tools to broadcast live from anywhere, at any time. All these factors turn the infosphere into an operational theatre for everyone, not just the military sphere.

In 1991, at the end of the Cold War, an analysis was conducted on approximately one hundred major armed conflicts that took place during that period. The conclusion was that the trend of demilitarizing warfare would intensify. The battleground would shift more toward the socio-spiritual, cultural, psychological, motivational, and emotional domains. The fight would aim at winning over the minds

and souls of the adversary's population, not just the fighters, through the manipulation of information, images, cultural elements, traditions, mentalities, interests, needs, and expectations. Over time, subtler and cheaper methods would be used to achieve strategic objectives, such as infiltrating centres of political, social, and media power, undermining and subjugating national economies, imposing value systems, altering public opinion, changing political regimes or leaders, and creating contradictions and fractures between governments and their populations (Arădăvoaice & Stan, 1999, p. 45).

Mass communication tools, especially television, have created what is known as video politics, a form of dependence comparable to an addiction (Postman, 1985, pp. 97-100). Control of the informational space depends significantly on the impact media networks have on the public. This also makes media networks powerful propaganda tools that facilitate psychological aggression. The mass media has become both a cause and a source of crises, amplifying the psychological warfare (psy-war) component of cyber-war through exclusive reports and revelations, which may or may not be real or credible. Psychological aspects of information warfare are not secondary but, on the contrary, are expected to gain importance in the future. For instance, the United States has developed specialized structures in the field of 3D warfare – disinformation, diversion, and destabilization (Nabila & Thompson, 2025, pp. 1893-1894). These involve missions aimed at destroying the enemy's media infrastructure while also broadcasting live events from operational theatres (Hentea, 1999, pp. 32-34).

It is well known that rumours, fabrications, insinuations, annotated press releases, exaggerations, threats, and various methods of intoxication, division, propaganda, disorientation, and disinformation – complemented by acts of

sabotage, crimes, political assassinations, and kidnappings – are all part of the preparatory phase of information warfare. This recalls McLuhan's statement: "*The new electronic interdependence recreates the world in the image of a global village*" (McLuhan, 1975, p. 68). Supporting this idea, contemporary events demonstrate that media networks indeed have the power to amplify conflicts or, conversely, to suppress them at their inception. A notable example is net war, conducted between governments or non-state actors, which highlights that we are in a third world war characterized by new forms of conflict – propaganda, cultural subversion, infiltration of observers, support for dissidents, actions by professional communicators and spies. These elements contribute to the ritualization of conflicts, maintained by media networks, as seen in examples like the Romanian tele-revolution (the fall of Nicolae Ceaușescu's regime was broadcast live on Romanian televisions) or the CNN war in the Gulf (in 1991, the first Gulf War was famously called the CNN War because it was the first war broadcast live, 24/7, around the world, The media turned warfare into a real-time spectacle, creating the sense of being there). Television, therefore, becomes a useful service primarily in times of crisis. We challenge McLuhan's statement that "*people do not accept war on television. In movies, yes. In newspapers, yes. But not on television. It is too close*" (McLuhan, 1975, p. 285). On the contrary, reality shows the public's appetite for sensationalism, violence, and bloodshed. The media network offers all of this through various means – print, audiovisual, and online platforms. Why? Because the most significant metric for mass media is audience ratings. Military-related topics tend to draw higher viewership in civilian media, which thrives on sensationalism, whereas the military press tends to be more objective.

Mass communication tools can easily become mass disinformation tools, with global consequences. Poor management of information circulating in media channels can influence various aspects of information warfare and, consequently, the behaviour of the conflicting parties. Of course, reactions in information warfare are not based solely on media-provided information, but media influence cannot be ignored. More than that, media networks are actively used to disrupt the adversary's information management and decision-making processes. One undeniable truth remains: mass communication tools are never 100% reliable and cannot guarantee the authenticity of information. Information warfare exploits precisely this uncertainty as a means of achieving its objectives.

6. Conclusions

While managing events within the dynamics of information warfare, military leaders must also consider the evolution of communication effects. Whether clandestine messages intended for disinformation and deception or desirable messages meant to inform, they must capture interest, seduce, shock, frighten, and attract – essentially, they must resonate with the audience. Theorists and practitioners of information warfare agree that these messages are predominantly visual because photographs, films, and television screens lend greater credibility to the message, embedding convictions. Warfare through imagery runs parallel to real conflict and can sometimes be just as victorious, as it is practically impossible today to imagine wars occurring without being broadcast live. Recent events in Egypt, Libya, and Syria over the past months demonstrate this reality, highlighting the impact that media networks have on warfare – not just information warfare, but conflicts in general.

From ancient intimidation and deception strategies, such as those

employed by Alexander the Great where forests were transformed into formations of armed soldiers – to modern propaganda methods based on low-tech approaches (pamphlets, radio and television broadcasts, and websites) and high-tech illusions (plastic sheet roads, inflatable tanks, cardboard bridges, and other stage props used in operations in the Gulf and Kosovo), all these elements of information warfare, built on manipulating information, are becoming defining characteristics of the new stage of informational confrontations.

Print media, audiovisual broadcasting, and the internet serve as tools that shape our consciousness beyond the limits of our own lives and senses. We have become dependent on media networks to stay informed about global events, with the immediate consequence being a heavy reliance on the credibility and integrity of information sources. Whether we like it or not, this dependence creates an opportunity for information manipulation – and, consequently, manipulation of the media audience and the people receiving these messages.

The relationship between mass communication and IW continues to be deeply intertwined, especially in today's digital age, where the specific channels serve as powerful tools for shaping public perception, influencing opinions, and disseminating information. These platforms become battlegrounds for manipulating narratives, often through disinformation, propaganda, or cyberattacks aimed at destabilizing societies or governments. Scientific research on the evolving character of conflict demonstrates that contemporary warfare is undergoing a paradigmatic transformation from a predominantly kinetic paradigm toward multidimensional, hybrid, and cognitive-centered forms of engagement.

Traditional military instruments, while not obsolete, are increasingly complemented – and in some contexts

supplanted – by cyber operations, information warfare, and disinformation strategies. These non-kinetic modalities enable adversaries to exploit systemic vulnerabilities, disrupt societal cohesion, and erode decision-making processes with a level of efficiency and deniability that conventional warfare cannot achieve. Consequently, the future security environment must be conceptualized through an integrated framework that acknowledges the convergence of physical, informational, and cognitive domains, emphasizing resilience, adaptability, and the safeguarding of democratic values in the face of hybrid threats.

This approach of our research intends to be continued by introducing another

aspect that plays a crucial role in this dynamic by enhancing the scale and sophistication of such tactics namely artificial intelligence (AI). AI technology, such as deep learning algorithms and natural language processing, can provide the creation and spread of misleading content, enabling the rapid and widespread distribution of false information, in an automatic way. It is one of the big challenges in this approach on the intersection between the communication tools and the IW, mostly because there is already a large conjunction with AI which could be a potent force in achieving strategic goals in warfare.

REFERENCES

- Alberts, D.S., Garstka, J., Hayes, R.E., & Signori, D. (2001). *Understanding informational age warfare*. CCRP Publication Series, 320. Available at: <https://roma.unuci.org/documenti/nwc/understandingInformationAgeWarfare.pdf>.
- Arădăvoaice, G., & Stan, V. (1999). *Războaie de azi și mâine. Agresiuni neconvenționale*. București: Editura Militară, 45-47.
- Arquilla, J., & Ronfeldt, D. (1997). Chapter *Cyberwar Is Coming!* In *Athena's Camp: Preparing for Conflict in the Information Age*. RAND, 23. Available at: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.
- Bakshi, B. (2018). Information Warfare: Concepts and Components. *International Journal of Research and Analytical Review*, 5(4), 178-185. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217782.
- Clausewitz C. (1982). *Despre război*. București: Editura Militară, 612.
- Drăgan, I. (2007). *Comunicare. Paradigme și teorii*. Vol. I. Rao, 286.
- Ducaru, S.D. (2016). The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO. *Europolity*, 10(1), 7-23. Available at: <https://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf>.
- Fiske, John. (2003). *Introducere în științele comunicării*. Polirom, 23.
- Fridman, O., Kabernik, V., & Pearce, J.C. (Eds.). (2019). *Hybrid Conflicts and Information Warfare. New Labels, Old Politics*. Available at: https://www.researchgate.net/publication/350632089_Hybrid_Conflicts_and_Information_Warfare_New_Labels_Old_Politics.
- Galeotti, M. (2022). *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press, 160-165. Available at: <https://doi.org/10.2307/j.ctv28bqm27.12>.
- Gilboa, E. (2016). Moving Media and Conflict Studies Beyond the CNN effect. *Review of International Studies*, Vol. 42, 661-662. Available at: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/9A53E5507A594F9AF4FF626BC4ACE9E9/S026021051600005Xa.pdf/moving-media-and-conflict-studies-beyond-the-cnn-effect.pdf>

- Hentea, C. (1999). Armata și presa. *Spirit militar modern*, Vol. 6, 32-34.
- Kuehl, D.T. (2002). Information Operations, Information Warfare, and Computer Network Attack. Their Relationship to National Security in the Infomation Age. *Internationale Law Studies*, Vol. 76, 50. Available at: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils>.
- Libicki, M. (1995). *What is Information Warfare?* National Defence University Press, 123-126. Available at: <https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf>.
- Mais, L.I. (2023). Media, Manipulation, and Information War. *Scientific and Theoretical Almanac Grani*, 26(5), 60-62. Available at: <https://doi.org/10.15421/1723102>.
- Maslen, S.C. (2024). *Hybrid Warfare under International Law*. Hart Publishing, 101-125. Available at: DOI:10.5040/9781509979608.
- McLuhan, M. (1975). *Galaxia Gutenberg*. Editura Politică, 68.
- McLuhan, M. (1997). *Mass-media sau mediul invizibil*. Editura Nemira, 285.
- McQuail, D. (1999). *Comunicarea*. Editura Institutul European, 173-174.
- Molander, R.C., Riddle, A.S., & Wilson P.A. (1996). *Strategic Infomation Warfare. A New Face of War*. RAND, 27. Available at: https://www.rand.org/pubs/monograph_reports/MR661.html.
- Mumford, A., & Pascal, C. (2013). Hybrid warfare: the Continuation of Ambiguity by Other Means. *European Journal of International Security*, 8(2), 193. Available at: <https://doi.org/10.1017/eis.2022.19>.
- Munteanu, N.A. (2009). *Exigențe ale libertății de exprimare prin mass-media*. Burg, 136-138.
- Munteanu, N.A. (2019). *Operația mass-media. Complementaritate a operației militare moderne*. TechnoMedia, 46-52.
- Munteanu, N.A. (2025). NATO's Mechanisms for the Governance of Cybersecurity. *Studia Securitatis Journal*, XIX (1), 209. Available at: <https://10.54989/stusec.2025.19.01.15>.
- Nabila, M.H., & Thompson, M. (2025). The Impact of Disinformation on National Security Policymaking: A Review. *EPRA International Journal of Multidisciplinary Research*, 11(6), pp. 1893-1894. Available at: <https://doi.org/10.36713/epra22781>.
- NATO (2024). *Countering Hybrid Threats*. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm.
- NATO. (2025). Cognitive Warfare. *NATO COGWAR Perception*, 1(1). Available at: https://www.act.nato.int/wp-content/uploads/2025/09/20250819_NU_CogWar_01.pdf.
- NATO Allied Command Transformation (2025). *Cognitive Warfare*. Available at: <https://www.act.nato.int/activities/cognitive-warfare/>.
- Postman, N. (1985). *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*. New York: Viking, 97-100.
- Rotaru, N. (2003). *Criză și dialog. Managementul comunicării de tip ierarhic*. Rao, 170-172.
- Sun, T. (2004). *Arta războiului*. Editura Samizdat, 10.
- Thompson, J.B. (2000). *Media și modernitatea*. Antet, 136.
- Toffler, A. (1983). *Al treilea val*. Editura Politică.
- Toffler, A. (1995). *Război și antirăzboi*. Antet.
- Topor, S., (2006). *Aspecte teoretice ale războiului informațional contemporan*. UNAP, 21.
- Turianu, C., & Pavel, D. (1996). *Calomnia prin presă*. Casa de editură și presă Șansa, 14-16.

Zeno-Zencovich, V. (2025). Speech as “Hybrid Warfare”. *Public Governance, Administration and Finances Law Review*, 10(1), 33-42, Available at: <https://10.53116/pgafnr.7939>.

Wolterman, J. (2019). *Mapping Information Warfare: Creating a Coherent Typology of Informational Coercion*. ISA, 10.

Wrobel, P.B. (2022). The Evolution of the Concept of Information Warfare in the Modern Information Society of the Post-Truth Era. *Defence Science Review*, Vol. 13, 48-62. Available at: <https://doi.org/10.37055/pno/152620>.

Zeca, C. (2002). Informația-factor de putere în războiul modern. *Gândirea militară românească*, Vol. 4, 44.