

DISINFORMATION AS A TOOL OF HYBRID WARFARE

Ionuț Alin CÎRDEI, Aurelian RAȚIU

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
cirdei.alin@armyacademy.ro, ratiu.aurelian@armyacademy.ro

Abstract: *Current conflicts are no longer carried out solely through the use of force, and the physical confrontation environment, characterized by the use of kinetic means, becomes a secondary confrontation environment, because the real confrontation takes place in other environments and has as its objective not the physical destruction of the adversary but the impact on the way of thinking and understanding reality. Under these conditions, the civilian population becomes a target of actions carried out in the physical and virtual environment, but also a powerful and efficient tool for achieving objectives and weakening the adversary. Hybrid warfare is multidimensional and aims to achieve effects in all areas and environments, using the most diverse means. Disinformation becomes, in the conditions of a fluid, dynamic, ambiguous confrontation environment, a basic tool that allows the achievement of general objectives and the shaping of the confrontation environment, without using armed force, aiming to influence the way of thinking of decision-makers and the population, decrease trust in the authorities and in their ability to manage complex situations, create panic, create a certain image of various state or non-state actors and direct support in certain directions.*

Keywords: hybrid war, disinformation, tool, influence

1. Introduction

The security environment is changing rapidly due to technological advances and the efforts of states and other relevant actors to reshape spheres of influence and reposition themselves on the international stage. Attempts to reshape the current world order and gain influence are hampered by regulations and agreements between states, and the use of force is not an option due to its implications and consequences, as highlighted by recent events.

Under current conditions, some actors of the international security environment have decided to employ hybrid strategies to achieve their security and foreign policy objectives, as these strategies yield excellent results with minimal international exposure and significantly lower costs relative to the benefits gained. Moreover, the use of hybrid means to achieve objectives renders the target unable to react or defend itself, as

these actions can only be identified very late, cannot be directly attributed, and are very difficult to counter, as they target not only physical infrastructure and the visible environment, but often aim to influence people's minds, their way of thinking, and their perception of reality.

By operating in a gray zone and selecting targets effectively, an actor who decides to gain an advantage or even threaten the security of another state by using hybrid threats as a tool will often succeed because he operates in a gray zone, shrouded in a specific fog, and seeks to reduce the target's ability to resist by using unconventional means and focusing on eroding public confidence in the state's ability to fulfill its functions, on undermining the credibility of legitimate actors and legitimizing the actions of hostile actors, and on changing the perception of the public and decision-makers regarding them.

The use of military means allows inflicting damage and defeating the adversary, but the use of hybrid tactics and strategies manages to cause greater harm without the use of physical force and without directly exposing the attackers: it allows one to influence people's minds and their perception of reality, thereby prompting them to behave in a certain way toward the state and its authorities, which serves hostile interests, without the affected individuals even realizing it.

In this context, "misinformation, disinformation and mal-information are currently very topical 'tools of choice' for the conduct of information warfare as witnessed in conjunction with COVID-19, Ukraine, and general elections in the Western World. These influence operations tools can be as destructive as kinetic operations, as they aim to distort, disrupt and undermine perceptions, political messaging and eventually and consequentially confidence in the Western rules-based system" [1].

Disinformation is becoming a tool specific to hybrid warfare, one that is used even in peacetime to sow discord and polarization within society, to erode public confidence in the state's ability to defend and promote their interests, and to weaken the state as a whole.

2. Disinformation – a tool for manipulating perceptions of reality and critical thinking

Of all the hybrid methods a hostile state or entity can employ, disinformation stands out as one of the most effective and easy to use because it spreads slowly, below the detection threshold, and has powerful and lasting effects, and the target is unaware that they are the victim of an attack, serving as a prime example of the "boiling frog" syndrome.

Due to the expansion of social media, which has established itself not only as a tool for communication and interpersonal interaction but also as a channel for

disseminating information that is increasingly replacing traditional media such as television, print and online newspapers, etc., a shift and improvement in the flow of information can be observed. However, this evolution has also highlighted the vulnerabilities of individuals, communities, and states regarding the use of social media and other information transmission channels for the purpose of altering or influencing behaviors and ways of thinking.

The struggle to control people's minds, direct their behavior, and influence their decisions is becoming increasingly intense, and the classic conflict, which involves the use of brute force to achieve objectives, is being replaced by a softer form of demonstrating power and influence, which has nothing to do with wealth, military power, political influence, or economic connections.

The widespread dissemination of misinformation poses a major global challenge, with profound implications for the public sphere, influencing both the dynamics of collective discourse and individual perceptions across a variety of fields, from health to politics.

Although often associated with the modern era, disinformation is not a new phenomenon; the deliberate use of false or misleading information for strategic purposes has accompanied the evolution of human society since ancient times. However, the rapid development of the digital environment has significantly amplified the pace and scale of disinformation campaigns, as well as the circulation of fake news. This transformation is driven by a number of factors, including the increased accessibility of content publishing, the ability to reach broad audiences, and the erosion of traditional mechanisms for filtering and verifying information, which previously helped maintain its credibility. Social media platforms have facilitated not only the proliferation of misinformation but also the

intensification of its impact on individuals and society as a whole. At the same time, these platforms provide the infrastructure necessary for conducting sophisticated disinformation campaigns through the use of fake accounts and bots—tools that are relatively easy to obtain and use. In this context, disinformation can be understood as an intentional and systematic process of distributing false or manipulated information, aimed at gaining political or economic advantages, while simultaneously generating negative effects on the public interest.

Disinformation is understood as “a set of information whose false or misleading nature can be verified, which is created, presented, and disseminated to obtain economic gain or to deliberately mislead the public, and which may cause public harm” [2]. Disinformation can also be defined as “the deliberate creation and spreading of false and/or manipulated information that is intended to deceive and mislead people, either for the purposes of causing harm, or for political, personal or financial gain” [3]. This scourge of the modern world is a component of the hybrid warfare waged by states or non-state actors against states or other competitors, using “a complex interaction of social media, online news sites, traditional media, and offline spaces” [4] to influence people’s thinking, to shape their behavior, to sow distrust, and to heighten anxiety.

Among the specific tools of hybrid warfare that are increasingly being used on the international stage, disinformation is becoming one of the most important instruments because, by leveraging modern means of information transmission and people’s dependence on the cyber environment, it manages to undermine their ability to think critically, induce certain feelings, and influence how they perceive reality, even creating a parallel reality in which nothing is what it seems, and truth becomes an extremely relative concept.

In recent decades, disinformation has emerged as a central tool in contemporary conflicts, particularly within the framework of hybrid warfare, where the boundaries between peace and war are becoming increasingly blurred and difficult to discern. In this context, military actions are no longer limited to the kinetic dimension but include a wide range of non-kinetic means designed to influence perceptions, alter decision-making processes, and undermine the adversary’s social cohesion. Disinformation, defined as the intentional dissemination of false or distorted information, plays a strategic role in achieving these objectives, serving as a low-cost, high-efficiency force multiplier.

In hybrid warfare, disinformation serves as a tool for shaping the information environment, contributing to the creation of a climate of uncertainty, mistrust, and polarization. This targets both the civilian population and political and military decision-makers, exploiting the cognitive and structural vulnerabilities of modern societies, such as dependence on digital media and the fragmentation of the information space. By manipulating narratives and amplifying sensitive issues, state and non-state actors can influence perceptions of the legitimacy of military actions, delegitimize the adversary, and reduce the adversary’s ability to respond coherently.

Disinformation is commonly used as part of the hybrid tactics employed by various states or interest groups because it allows them to achieve their objectives with minimal effort and erodes public trust in state institutions, amplifies societal polarization and divides society into opposing camps, beyond the specific bubbles of the internet and social media, it accentuates existing social divisions and, in the medium and long term, affects the government’s ability to fulfill its core tasks, provide security and stability to citizens, increase the population’s well-being, and ensure optimal conditions for development. Taken to the extreme,

disinformation can “lead to radicalization and violence, can cause doubt, confusion, and frustration, and its presence can make it harder for people to find and trust accurate information” [5]. Once the seed of distrust has been sown among the population, it will spiral into a culture of conspiracy theories, and people will no longer trust anything associated with the state or the authorities; instead, they will seek out only those messages and information that support their point of view and validate their theories and beliefs.

Disinformation is not spread by hostile states or entities using the instruments of state power; rather, they employ a variety of methods and means tailored to the times we live in and the way people perceive reality. Thus “disinformation ecosystem is diverse, encompassing official state entities, state-funded media outlets, proxy organisations, ideologically-driven individuals and commercially-motivated journalists and bloggers” [6], each of these having its own methods, its own target audience, and greater effectiveness within its specific field. If these tools are used as part of a complex strategy to manipulate perceptions and the way people think, their effectiveness will be maximized because they will create synergistic and lasting effects on society and make it very difficult to counteract disinformation and identify its source.

Disinformation campaigns are highly effective because they are designed to create confusion and polarization and to amplify feelings of fear and mistrust. In everyday life, anyone can be a target of disinformation campaigns, and to avoid becoming a victim or a vector for spreading disinformation, everyone must maintain a high level of awareness and sufficient media literacy, develop critical thinking skills, and strengthen their security awareness. People can fall victim to disinformation if the false information they encounter aligns with their preexisting values and beliefs, if it elicits an emotional response due to the way the facts are presented, if it is disseminated by

individuals who enjoy a certain degree of credibility, if exposure is repeated and prolonged, and if the online bubble in which they operate fosters feelings of distrust toward authorities or even hostility toward them [4].

Social media platforms are designed to exploit users' emotions, and the way they operate allows for the rapid and indiscriminate spread of messages that exploit people's emotions because “the more volatile and divided a society is in political and social aspects, the more vulnerable it is to disinformation” [7].

The spread of false information and the conduct of disinformation campaigns are amplified by the use of bots, fake accounts, and artificial intelligence in general, which automate the dissemination of information and increase the likelihood that it will reach the most vulnerable users.

Ordinary people, however, are not merely targets of misinformation; they can actually become vectors that spread false information and amplify these messages for various reasons, such as: the fact that they believe this information and consider it useful to share it, carelessness, lack of knowledge, the desire to belong to a group, the desire to be the center of attention and feel important, the desire to spark a debate or initiate a discussion on a topic of interest, the attempt to gain social validation, to provoke an emotional response, the desire to cheer others up, or even the intention to cause unrest and chaos.

An interesting aspect of disinformation is that once a disinformation campaign is launched, false information spreads like a snowball, gaining momentum and becoming increasingly difficult to stop and counteract. People unwittingly become tools through which this scourge spreads and even come to believe that their actions are completely justified, which turns them into “useful idiots” who unconsciously serve a cause that is harmful to society and even to themselves.. Once a message enters the information ecosystem, it will spread

rapidly, go viral, and become increasingly difficult to counter.

Disinformation campaigns are carried out with the aim of influencing what other people think or feel, or to influence their decisions. When these actions are carried out in a coordinated manner, across multiple platforms, targeting various audiences, and employing diverse methods to achieve their objectives, we are witnessing the emergence of full-fledged disinformation campaigns, which constitute a key component of hybrid warfare operations, and disinformation stands out as a subversive tool used to destabilize the adversary, to reduce its domestic support, and to mobilize the population's energies to weaken the target state and legitimize the attacker's actions.

Moreover, disinformation is not used solely against the civilian population or in peacetime; rather, it is a means of weakening the adversary and achieving economic, political, or military objectives even during times of conflict. The use of disinformation in military operations is not a new phenomenon, but recent technological developments have significantly amplified its scope and speed of propagation. Digital platforms and social media facilitate the rapid dissemination of manipulative content, enabling the conduct of complex information operations synchronized with conventional military actions. Thus, disinformation becomes an integral part of the planning and execution of military operations, contributing to the attainment of strategic advantage by influencing the adversary's cognitive environment.

Therefore, analyzing disinformation as a tool of hybrid warfare highlights the need for a thorough understanding of the informational dimension of contemporary conflicts. Its integration into military strategies signals a paradigm shift, in which control over information and perceptions becomes just as important as traditional military superiority.

3. Considerations on countering disinformation

Disinformation is a constantly evolving threat that affects all sectors of society in different ways. When it is part of a coordinated campaign aimed at undermining the state's interests and weakening its ability to perform its core functions, it can be said to constitute the non-kinetic component of an ongoing war. "The impact of the spread of disinformation and hoaxes on social media is diverse and can affect various aspects of people's lives, from influencing public opinion and disrupting the democratic process to causing social unrest and threatening national security. In the context of national security, disinformation and hoaxes can be used as tools to manipulate public perception or trigger conflict and may even serve as weapons in information warfare between countries" [8]. Therefore, efforts to counter disinformation and limit its effects must be part of a broader plan that includes national authorities, journalists, traditional and online media, as well as the general public, who must become partners with the authorities in this fight. Combating hybrid warfare is not merely the responsibility of the state, but rather a responsibility of society as a whole, because in one way or another, society as a whole suffers as a result of it.

Countering disinformation, in particular the one that spreads online, is "a global issue that affects all democracies and requires a response from all areas of society—governments, industry, civil society and citizens" [5].

Countering disinformation involves using all available legal means, without infringing upon citizens' fundamental rights and freedoms, and requires efforts not only from state authorities but also from opinion leaders, people who enjoy credibility, and ordinary citizens who understand the importance of their personal contribution to the common good and who can counter the spread of disinformation through their individual actions.

To effectively combat disinformation, authorities must adopt a consistent strategic approach that takes into account the country's internal characteristics, the specificities of its population, the ways in which misleading messages and false information spread, and the presumed purpose of such campaigns. Furthermore, authorities must be aware that there are no miracle solutions or universally applicable methods for combating disinformation; therefore, each situation must be assessed individually to identify the best course of action.

The fight against disinformation has also come to the attention of the European Union, which has identified a series of general principles and objectives to guide efforts to combat disinformation, such as [2]: "improving transparency regarding the origin of information and how it is produced, sponsored, disseminated, and targeted, to enable citizens to evaluate the content they access online and to identify potential attempts to manipulate public opinion; promoting diversity of information to enable citizens to make informed decisions based on critical thinking, by supporting high-quality journalism, media literacy, and rebalancing the relationship between information creators and distributors; promoting the credibility of information by providing an indication of its reliability; developing inclusive solutions". Effective long-term solutions require public awareness, better media literacy, the involvement of as many stakeholders as possible, and cooperation between public authorities, online platforms, advertising agencies, journalists, and media groups. The European approach is based on building a partnership between authorities and citizens so as to prevent the creation of a fertile ground on which disinformation can emerge and spread. This approach also encourages the development of individual and societal resilience in the face of hybrid threats in general and against disinformation in particular.

Building resilience is a long-term process, the effectiveness of which will only become apparent in times of crisis, and it requires ongoing efforts in several areas, such as [5]:

- sharing accurate information with the public as early as possible through trusted channels and communicators;
- supporting the development of digital literacy;
- demonstrating openness and transparency in all situations to foster a climate of mutual trust;
- engaging the core audience as frequently as possible with accurate messages tailored to the situation and the audience's characteristics;
- acknowledging aspects that are unknown or about which there is insufficient information;
- combating fake news and the communicators of such news;
- promptly refuting false information and providing clarity in the public sphere;
- creating platforms/databases containing false information and effectively countering them (such as the EU vs. Disinfo platform);
- proactive communication, especially in tense situations;
- conducting public awareness campaigns;
- using experienced, credible, and high-profile communicators;
- exposing and punishing those who use disinformation to harm citizens' interests or national interests;
- strengthening the state and the legal tools at its disposal to deter future actions.

Measures to strengthen resilience must be part of a more comprehensive strategy to counter disinformation that involves state resources and is structured across multiple lines and areas of action to strengthen the capacity of the state and the population to cope with disinformation. The authorities'

response to disinformation must consist of both passive and active measures that enable the identification, countering, and even sanctioning of aggressive actors and the networks behind disinformation. [9].

Public communication is crucial for building trust between the public and state, which enhances the legitimacy of decision-makers and helps ensure that differences of opinion do not lead to major divisions in society [10]. To achieve these goals, it is necessary to develop an information environment that promotes transparency, allows for the verification of sources and the accuracy of information, and encourages accountability in ensuring fact-based public communication.

Combating disinformation transcends the borders and interests of individual states. That is why, in addition to the efforts undertaken by the European Union, we can also point to NATO's actions in this regard, for which "tackling disinformation remains an essential part of the communication strategies and day-to-day operations, which includes media monitoring, analysis of the information space and proactive communication in a coordinated and fact-based manner" [11].

6. Conclusions

Disinformation is a phenomenon that has essentially spiraled out of control due to the public's unlimited access to numerous sources of information that cannot be verified and that can be manipulated by malicious actors. In the online environment, and especially on social media platforms, coordinated disinformation campaigns can be organized because specific algorithms allow for targeting segments of the population that are susceptible to these tactics and can even bombard a very large number of people with false information that appears highly credible. Since people live in online bubbles, it is very important for attackers to penetrate these bubbles, and once inside, they will be able to spread their messages using various vectors and even

"useful idiots," because some people, once they find a cause, begin to promote those ideas out of pure conviction, without realizing the consequences of their actions. Tools of disinformation in the online environment can include bots, specially designed algorithms that exploit vulnerabilities and identify affinities, troll farms, deepfakes, as well as other means that exploit people's psychological vulnerabilities, their desire for recognition, their need for validation, etc. Generative AI is already being integrated into disinformation operations. Automated tools generate fake articles, social media posts, images and deepfakes [6].

Disinformation takes advantage of the benefits offered by technology and exploits the opportunities provided by social media to ensure that false or heavily distorted information reaches as many people as possible who are no longer able or willing to critically assess this infodemic. In many cases, social media facilitates the spread of disinformation because bots are used to amplify messages, strong emotions are created and exploited to motivate people to participate in spreading the message, and the speed at which information is transmitted and a visible effect is achieved is very high. Moreover, once released, this message spreads infinitely through repeated sharing, and its source cannot be traced, making it extremely difficult to counteract disinformation. People are highly vulnerable to disinformation due to their appetite for sensationalism and their trust in information circulating online, and literacy rates—especially information literacy—are very low. Furthermore, the fact that society is polarized and trust in state institutions is constantly eroding creates fertile ground for the spread of disinformation, with unforeseen consequences for individuals, communities, and states. This undermines public confidence in the state's ability to fulfill its basic functions, casting doubt on the state's integrity of the state in relation to its citizens and ultimately undermining

national security, reducing social cohesion, and eroding trust in state institutions, democratic processes, and the economy. The lack of a culture and education in this area allows those behind disinformation campaigns to exploit people's fears and vulnerabilities, amplify their anxiety and mistrust, fuel aggressive and antisocial sentiments, opinions, and behaviors, and create the conditions for discontent and chaos to arise.

Building individual, organizational, and societal resilience can be a solution to combating disinformation and requires collaboration and engagement among central authorities, opinion leaders, and local authorities, as well as the development of trust-based relationships between citizens and authorities. Creating and developing a culture of expertise, digital literacy,

combating illiteracy, etc., can be measures that contribute to increasing resilience against disinformation.

Western countries address the issue of disinformation and how to combat it in different ways due to differences in history, culture, national and regional security, education, the quality of the media, the level of public trust in authorities, traditional relations with states or actors perceived as sources of disinformation, etc., however, in all countermeasures, it must be borne in mind that individual rights and freedoms must be protected, and their restriction must be an exceptional measure, in exceptional situations and for limited periods of time, which may affect the effectiveness of measures to counter disinformation.

References

- [1] Sascha-Dominik Dov Bachmann, Dries Putter, Guy Duczynski, Hybrid warfare and disinformation: A Ukraine war Perspective, Global Policy. 2023;00:1–12, available at: <https://doi.org/10.1111/1758-5899.13257>.
- [2] Comisia Europeană, Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, Combaterea dezinformării online: o abordare europeană, Bruxelles, 26.4.2018, COM(2018) 236 final, available at: <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52018DC0236>.
- [3] Cabinet Office, Government response. Fact Sheet on the CDU and RRU, available at: <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru>.
- [4] Eva Surawy Stepney, Clare Lally, Disinformation: sources, spread and impact, 25 April 2024, available at: <https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf>.
- [5] Government of Canada, Countering disinformation: A guidebook for public servants., 2024.
- [6] Claudia Wallner, Simon Copeland, Antonio Giustozzi, Russia, AI and the Future of Disinformation Warfare, Royal United Services Institute for Defence and Security Studies, 2025.
- [7] Horowitz Minna Aslama, Disinformation as warfare in the digital age: dimensions, dilemmas, and solutions, 2019, Journal of Vincentian Social Action: Vol. 4 : Iss. 2 , Article 5., p. 9, available at: <https://scholar.stjohns.edu/jovsa/vol4/iss2/5>.
- [8] Dwi Surjatmodjo, Andi Alimuddin Unde, Hafied Cangara, Alem Febri Sonni, Information Pandemic: A Critical Review of Disinformation Spread on Social Media and its Implications for State Resilience, Social Sciences 13:418, 2024, available at: <https://doi.org/10.3390/socsci13080418>.
- [9] Jakub Kalenský, Heidi Hanhijärvi, Hybrid CoE Research Report 15 Countering disinformation in the Euro-Atlantic: Strengths and gaps, September 2025.

- [10] Stormy-Annika Mildner, Alyssa McIntyre, and Niklas Zimmer (eds), Hybrid Realities: Disinformation, Influencers, and the Defense of Democracy in Central and Eastern Europe, publisher Aspen Institute Deutschland e.V., December 2025.
- [11] Tomasz Chłoń, NATO and Countering Disinformation. The Need for a More Proactive Approach from the Member States, 16 May 2022, p. 6, available at: <https://www.globsec.org/what-we-do/publications/nato-and-countering-disinformation-need-more-proactive-approach-member-0>.