Natalia Putină*

STRENGTHENING THE RESILIENCE OF STATES AGAINST HYBRID THREATS – LESSONS FOR THE REPUBLIC OF MOLDOVA

CZU: 351.86:004.056.5(478) **DOI: https://doi.org/10.5281/zenodo.12719755**

Abstract

Hybrid threats have become an increasingly frequent and pressing topic in the agendas of states and international organizations regarding national, regional and global security. Challenges from state or non-state actors, aimed at exploiting the vulnerabilities of political systems to their own advantage, through the use of an amalgam of diplomatic, military, economic, and technological instruments, are quite frequent.

The research comes to analyze the policies and actions taken by the authorities of the Republic of Moldova in order to counter the hybrid threats that our state is facing. States are responsible for responding to hybrid threats by enhancing their resilience and by detecting, preventing and responding to hybrid threats. In the development and planning of responses to hybrid threats, the Republic of Moldova must also focus on the solutions offered by the EU institutions in providing coordinated responses to the entire community, starting from actions aimed at raising awareness of the situation; increasing information security resilience in the segments of maximum vulnerability and increasing response capabilities.

Keywords: *hybrid threats, information security, disinformation, propaganda, EU accession, hybrids, information security, disinformation, propaganda, EU accession*

Understanding the concept of hybrid treatments and its levels of implications in contemporary societies

The conclusion of the Cold War and contemporary global political shifts have brought about a transformation in the obstacles and hazards facing states in their pursuit of peace, prosperity, and security. These challenges have extended into new domains where both state and non-state actors are involved, necessitating a reevaluation of the traditional notion of security and international cooperation. Present-day hybrid threats surpassing the military sphere are prevalent and comprise of conventional and unconventional methods employed to achieve political and strategic objectives. In response, states and international organizations have been compelled to redefine their approach towards security and devise innovative means of working together (Review Intelligence, 2017a).

*Associate prof., Moldova State University, natalia.putina@usm.md, https://orcid.org/0000-0002-3607-4103

The European Union has adopted the term "hybrid threats" as its preferred terminology, as it is considered more diplomatic than technical or analytical. The EU's diplomatic culture does not allow for the official use of the term "hybrid war" because it implies that the EU is at war with Russia or other states utilizing hybrid aggression against them. However, the term "threat" is not accurate analytically. A threat refers to a potential cause of harm resulting from intentional or unintentional actions (Patryk Pawlak, 2015). ” Hybrid threats” are realized by state or non-state actors, having as their main purpose to produce harm and to influence its decision-making at the local, regional, state or institutional level, by targeting democratic states and exploring institutions’ vulnerabilities. The conducted activities may attempt on political, economic, military, civil or information areas, having a wide range of instruments designed to remain below the threshold of detection and attribution. Hybrid treats has an ambiguous character and operate by blurring external, internal, legal and illegal, peace and war borders of politics

Hybrid actions combine conventional and unconventional forms of influence such as disinformation and intervention in political debate or elections, critical infrastructure disruptions or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare (Daniel Fiott, 2022, https://www.hybridcoe.fi/). I t is associated with actions that have yet to occur but are anticipated. For example, we can discuss the threat of artillery strikes before they happen, but once the artillery attack commences, it is no longer a threat but an attack. Given that the elements of hybrid war are already evident in Moldova, Ukraine, and other countries, we must address actions rather than threats. It is not appropriate to use the term "threat" when an attack has already occurred, based on the hybrid war model in use (Mînzărari, 2021, 9-10).

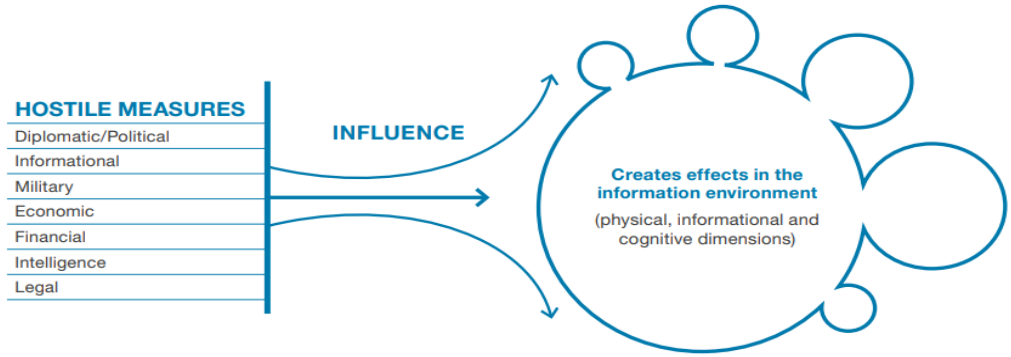
Hybrid actors employ both unconventional and conventional means together to obscure their actions and make attribution and response difficult, utilizing proxy actors to achieve their goals. This approach is cost-effective, as it allows the vulnerabilities of the target to be turned into a strength for the hybrid actor. The ongoing shift in global power dynamics creates an ideal environment for hybrid action, as the conflict between Western and authoritarian values undermines international norms and institutions, leaving open societies vulnerable to comprehensive hybrid attacks. Moreover, this conflict of values has extended into Western domestic spheres, increasing polarization and disunity among Western actors and making them more susceptible to external interference (Hybrid CoE, https://www.hybridcoe.fi/).

Recent advances in technology and the increasingly complex information environment provide hybrid actors with potent tools, which can be exploited to great effect if not properly countered. The Hybrid CoE describes hybrid threats as coordinated and synchronized actions that

deliberately target the systemic vulnerabilities of democratic states and institutions through various means. These activities exploit the thresholds of detection and attribution, as well as the different interfaces between various security realms. The end goal of these actions is *to influence decision-making at the local, state, or institutional levels, in order to further the agent's strategic objectives while simultaneously undermining or harming the targe*t. (Hybrid CoE, https://www.hybridcoe.fi/)

Hybrid threats can therefore be considered as information or influence activities. These are actions which influence audience perception and decision-making. Such activities are not limited to the 'Information' instrument but involve the combination of different instruments of power, including Diplomatic, Economic and Military.

Figure 1. Haw hybrid treats influence the information environement



Source: *Hybrid Threats. A Strategic Communications Perspective*, NATO StratCom,COE, https://stratcomcoe.org/cuploads/pfiles/2nd_book_short_digi_pdf.pdf

First, in 2005, two senior US military officials discussed the "rise of hybrid wars," emphasizing the combination of conventional and unconventional strategies, methods, and tactics in modern warfare, as well as the psychological or information-related aspects of modern conflicts. Second, Russia invaded Crimea in 2014 and achieved its goals by combining "deniable" special forces, local armed actors, economic clout, disinformation, and exploitation of Ukraine's socio-political polarization (Bilal, 2021).

Although, after the annexation of Crimea, the main ideologue of the "hybrid war" was considered the Chief of Staff of the Russian Army, General Valeri Gerasimov, in the academic and analytical environments this type of conflict is not considered a novelty. His conceptualization is increasingly attributed to the Russian military theorist Yevgeny Messner (1891-1974), colonel of the General Staff of the Tsarist army, known as the author of the phrase ”meatejevoina” ("war of insurgency" or "insurrectionary war").

According to the Albgardist officer, the Bolsheviks set up a new kind of war, the “meatejevoina” in order to challenge and possibly defeat the West,

without fear of triggering a direct military confrontation. Describing this type of conflict, the Russian theorist draws attention to the absence of peace-war dichotomy and a classical line of the front, as well as the domination of the psychological component (Review Intelligence, 2017b). Both in the official Russian rhetoric and in the text of the main programmatic documents of the Russian Federation (such as the Military Doctrine, the Doctrine of Information Security, and the Foreign Policy Concept) the term "hybrid" is not used, the phrases "war of the future", "asymmetric threats" and "measures to counter the color revolutions" are preferred (Review Intelligence, 2017b).

Critics often oversimplify the goal of hybrid war by assuming that *its aim is to persuade a sympathetic population to comply with the aggressor's wishes, such as supporting the aggression or remaining neutral.* However, this view is overly simplistic. In reality, the population-centered aggression mechanism offers several choices, including:

- *convincing a loyal ethnic group to support the aggressor's preferred policies*, which may involve opting for military neutrality or forging closer ties with Russia;
- *directing a critical segment of the population*, which may be hostile to the aggressor*, to oppose a policy that the aggressor dislikes;* and
- *creating significant social divisions within a society by inciting certain segments of the population to challenge or threaten other groups*. This may involve stoking separatism, religious or ethnic tensions, or political polarization (Mînzărari, 2021: 10).

Disinformation and hybrid warfare

After Voicu „fake news„ creates distortions in the social structure. Fake news has become the engine of a new reality, the expression of a new era, that of post-truth. The military sees here a new expression of hybrid warfare, academia talks about informational pollution, and philosophers talk about a new paradigm of communication, while psychologists identify a new type of mental disorder - informational disorder (Voicu, 2018, p. 18)

Considering the current situation, media experts have suggested new concepts that can provide a more neutral, clear, and comprehensive description of the ongoing process. These concepts include "disorder" or "information dysfunction" (the term "information disorder" was used in a 2017 report by the Council of Europe entitled "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making").

To elaborate, three types of information have been identified:

- *disinformation,*
- *misinformation, and*
- *mal-information.*

We therefore introduce a new conceptual framework for examining information disorder, identifying the three different types: mis-, dis- and mal-information. Using the dimensions of harm and falseness, we describe the differences between these three types of information:

- *Mis-information is when false information is shared, but no harm is meant.*
- *Dis-information is when false information is knowingly shared to cause harm.*
- *Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere* (Wardle, Claire, Derakhshan, Hossein, 2017).

Disinformation and misinformation are commonly used and encountered terms that refer to false or misleading information or content, with the primary difference between them being the subjective side or intended purpose. *Misinformation* is intentionally and repeatedly spread to deceive or cause harm, whereas disinformation is not disseminated with the intention of causing harm. Mal-information, on the other hand, refers to the dissemination of true information (often private or exaggerated) that is used to mislead or cause harm (Review Intelligence, 2023).

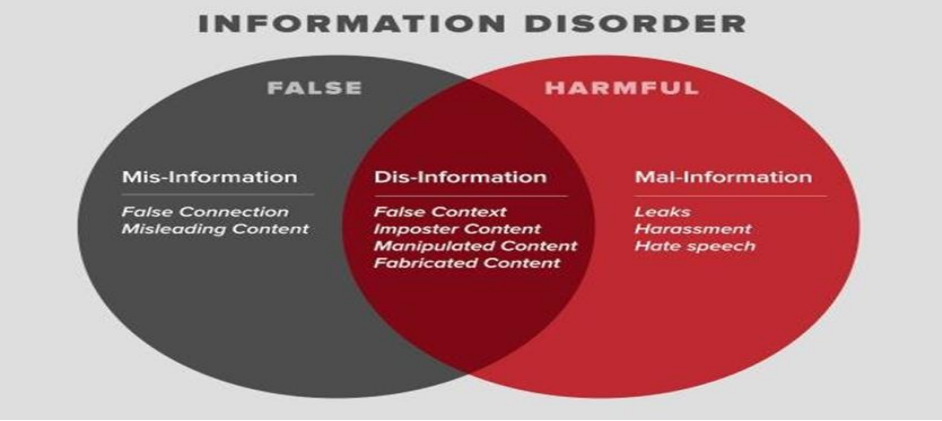
Disinformation is most effective when agitating existing social divisions in society. Social divisions are often rooted in individual and societal assumptions and prejudices linked to identity markers like gender, race, class, ethnicity, sexual orientation, or age. These identities often play a central role within existing wedge issues, or issues of conflict in societies (Freedman, 2021). Disinformation campaigns often target social identities that reflect power relations between people in society, and between dominant and non-dominant groups (Hoogesen, 2006).

Disinformation targets people's emotions, particularly negative emotions like hate, disgust, anger, fear, and sadness (Oliveira, 2023). Emotional narratives are powerful tools, and the messaging is often tailored to a particular audience. The adversary tries to identify the most divisive topics where it is easiest to evoke strong emotions, and these topics vary from one audience to another (Kalensky, 2022). In the US, it might be a matter of divisive racial narratives (Barnes, 2020), whereas in many Central and Eastern European countries, one often encounters disinformation about migrants and refugees (EuvsDisinfo, 2021) 13 or anti-LGBT messaging, such as narratives about "gay Europe" versus countries where traditional values and masculinity are typically favoured. The norms around these identities are closely linked to statebuilding: how we govern, who has the power to govern, and who sets the governing agenda (EuvsDesinfo, 2019).

The Anti-propaganda website studied daily news broadcasts of the main Russian TV channels, quantifying the percentage of what it deemed propaganda. The April 21st broadcast of the program "Vesti" on the Russia24

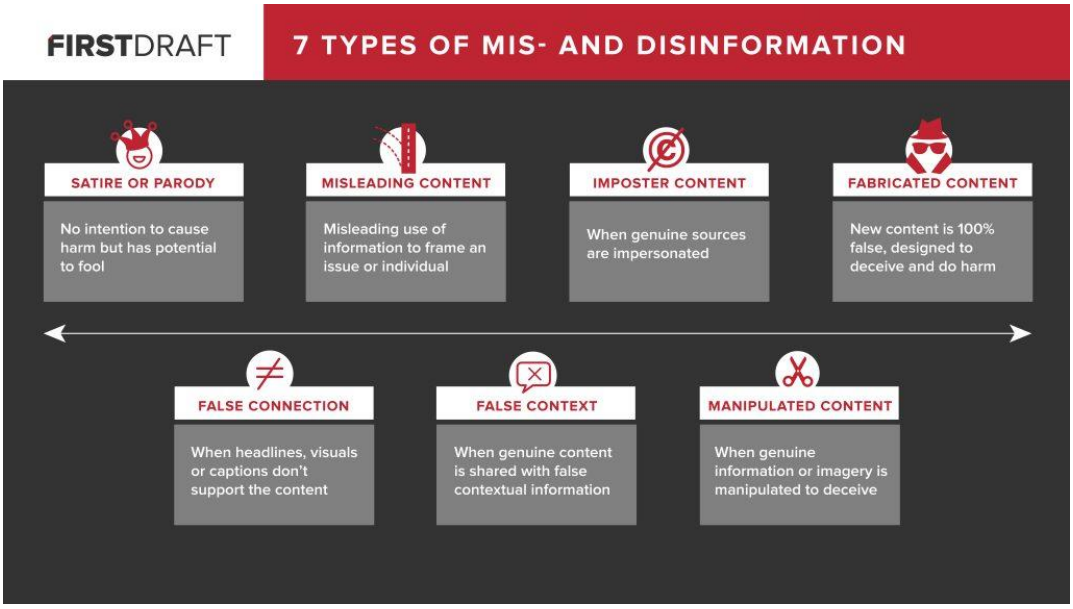
channel, for example, was listed as “66% propaganda.” Each program was described in detail, along with quotes by the anchormen or women and a list of propaganda techniques used, e.g. demonization of the enemy,” “disinformation,” “oversimplification,” and “substitution of facts with opinions” (Cole, Robert Cole and his book, The International Encyclopedia of Propaganda). Propaganda or not, viewers in Russia who watched the broadcasts were primed to accept the government’s narrative that Nazis had carried out the uprising in Kiev (Dougherty, 2014, p.5-6).

Figure 2. Information disorder



Sourse: Wardle, Claire, Derakhshan, Hossein (2017) *Information Disorder: Toward an interdisciplinary framework for research and policymaking,* Report Council of Europe, October, 2017. www.coe.int, https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/

Figure 3. Types of Mis-and Dis-information



Source: Wardle, Claire, Derakhshan, Hossein (2017) *Information Disorder: Toward an interdisciplinary framework for research and policymaking,* Report Council of Europe, October, 2017. www.coe.int, https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/

While misinformation is not a new phenomenon, the rise of the internet and social media has brought about significant changes in how information is produced, communicated, and distributed. Some of the key characteristics of the modern information environment include:

- The availability of widely accessible, affordable, and sophisticated editing and publishing technology has made it easier for anyone to create and distribute content.
- The private consumption of information has become more public due to the use of social media.
- The speed at which information is disseminated has been amplified by an accelerated news cycle and the use of mobile devices.

Information is rapidly shared among trusted peers in real-time, making it less likely to be challenged or scrutinized for accuracy (Wardle, Claire, Derakhshan, Hossein 2017).

As we have seen, the dynamics of the security environment are changing and if until recently, elements related to military threats were treated as such, the infusion of these elements into the civilian area can be due to hybrid warfare and the threats they generate. Thus, defining and offering some concepts operational to clarify the role and significance of information warfare and a information operations, together with its components, become essential. Considering the current context, in which the confrontations in the informational environment no longer distinguish between a state of peace and war, it becomes imperative that states clarify their concepts and develop their own information strategies and weapons – as in the case of conventional armaments and doctrines –, whereby to gain advantages, protect themselves or limit the opponent's opportunities (Putină, 2022, p.137).

The current security environment in the Republic of Moldova: vulnerabilities and threats

At present, the Republic of Moldova does not have the necessary mechanisms for the identification and prevention of hybrid threats, nor for the development of tools to protect against hybrid warfare. The national debate on hybrid threats and wars remains largely limited by the lack of in-depth analyses, which would address the size and complexity of future risks for the Republic of Moldova (Sterpu, 2021, p.5).

Hybrid security threats can represent a significant concern for the Republic of Moldova in the context of its accession process to the European Union (EU). Hybrid threats are combined actions or tactics that use a variety of means, including information warfare, propaganda, influencing domestic political processes, disinformation, undermining institutions, and others, to

weaken the integrity and sovereignty of a state. In the case of the Republic of Moldova, these threats can have the following dimensions:

- *Information warfare and disinformation*: Russia has used propaganda and disinformation in the past to influence public opinion in the Republic of Moldova and undermine trust in government institutions. These actions can weaken support for EU membership and distort public discourse.
- *The Transnistrian conflict:* The separatist region of Transnistria, supported by Russia, is a source of constant tension in the Republic of Moldova. This instability may hinder progress towards EU membership.
- *Corruption and institutional fragility*: Corruption remains a major problem in the Republic of Moldova and can undermine the democratic processes and reforms needed to meet EU requirements. Corrupt interest groups can be used as tools for foreign influence.
- *Internal political divisions:* Political divisions in the Republic of Moldova can be exploited by external actors to undermine reform efforts and block progress towards EU membership.
- *Energy dependence:* The Republic of Moldova depends on the supply of energy from Russia. This dependence can be used to exert political and economic pressure on the country.
- *Labor migration:* The massive emigration of labor from the Republic of Moldova can have a negative impact on the country, both economically and from the perspective of the human resources available to support the reforms.

To deal with these hybrid threats, the Republic of Moldova needs to strengthen its institutions, consolidate democracy and work to diversify its foreign relations and energy sources. Also, international support, especially from the EU, can play an essential role in supporting security and reform efforts in the Republic of Moldova. It is crucial that the Republic of Moldova maintains its determination to join the EU and continue its efforts to overcome these hybrid threats.

Moldova participated in the 59th Security Conference in Munich, Germany, on February 17-19. The Delegation of the Republic of Moldova led by President Maia Sandu also includes the Minister of Internal Affairs, Ana Revenco. The conference tackled topical topics, including: strengthening the resilience of the Republic of Moldova and the state of security in the region, hybrid threats from the Russian Federation, as well as the perspectives and priorities of cooperation with the Member States of the European Union (zugo.md 2023)

In order to combat hybrid threats and to strengthen its security, the Republic of Moldova adopted a series of normative acts and took measures in recent years. One of the latest public policy document is the National Security

Strategy, 2024. The new Draft of National Security Strategy of the Republic of Moldova comes as a response to new trends, with benign and malignant character, in the field of security. The strategy provides a guide for adapting to the evolving security environment transformation, to effectively combat a whole range of challenges, but also an exploit regional and global opportunities in order to ensure sustainable a national security interests. The main strategic orientations of the document represent.

- *to define national security interests,*
- *to establish the principles that guide the effort to promote and defend National Security 'interests,*
- *to escribes the elements of the global and regional security environment that are relevant for national security,*
- *to identify the range of threats, risks and vulnerabilities at risk national security,*
- *to establishes the methods and outlines the directions of action in order to prevent, minimizing or neutralizing challenges* to national security.

The strategy addresses national security comprehensively and multidimensional, in terms of both the diverse nature of security challenges faced by the Republic of Moldova, as well as the variety of actions coordinated on several plans, necessary to combat or prevent them.

Conclusions and recommendations

The Republic of Moldova should develop strategic communication capabilities to counter foreign propaganda and communicate effectively with its citizens and international partners.

The Republic of Moldova should collaborate with international partners, especially the European Union and the North Atlantic Treaty Organization (NATO), to receive support and technical assistance in addressing these threats. It is important to maintain an open dialogue with international partners and monitor global developments regarding hybrid threats and adapt strategies accordingly.

Building trust of state institutions is indeed crucial in combating hybrid threats, as it helps to prevent their intended polarization and erosion of core values. Trust can be built through various means, such as promoting transparency, accountability, and effective communication between governments and citizens.

Governments must also demonstrate their commitment to democratic values and the rule of law by respecting human rights, ensuring free and fair elections, and protecting the independence of the media and judiciary. Moreover, trust-building efforts must extend beyond the national level to include international cooperation and collaboration.

BIBLIOGRAPHY

Arsalan Bilal, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, 30 November 2021

Barnes, Julian E. et al., 'Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say', The New York

Cole, Robert (1998) International encyclopedia of propaganda, London : Fitzroy Dearborn

COVID-19 News', SN Comput Science, Volume 4, Article 11, (2023).

De la fake news la dezordinea informațională, in: Revista Intelligence, 25 ianuarie 2023, https://intelligence.sri.ro/de-la-fake-news-la-dezordinea-informationala/

Dougherty, Jill (2014), Everyone Lies: The Ukraine Conflict and Russia's Media Transformation, Shorenstein Center on Media, Politics and Public Policy, Discussion Paper Series, #D-88, July 2014, https://shorensteincenter.org/wp-content/uploads/2014/07/d88-dougherty.pdf

EUvsDisinfo, *Greasing the Wheels with Disinformation: Migration and NATO in the Focus of the Pro-Kremlin Media', 25 November, 2021,* ttps://euvsdisinfo.eu/greasing-the-wheels-with-disinformation/

EUvsDisinfo, 'Russophobia, Dependence, and the Belarusian Gay-Opposition', 4 July, 2019,

Fiott, Daniel Hybrid CoE Paper 13: *Digitalization and hybrid threats: Assessing the vulnerabilities for European security*, 2022, https://www.hybridcoe.fi/publications/hybrid-coe-paper-13-digitalization-and-hybrid-threats-assessing-the-vulnerabilities-for-european-security/

Freedman, Jane et al., 'Identity, stability, Hybrid Threats, and Disinformation' ICONO, Volume 14, Issue 19,

Hoogensen, Gunhild et al., Gender, Resistance, and Human Security, in *Security Dialogue,* Volume 37, Issue 2, https://euvsdisinfo.eu/russophobia-dependence-and-the-belarusian-gay-opposition/;

Hybrid CoE, *Hybrid threats as a concept*, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/#:~:text=The%20use%20of%20different%20intermediaries,to%20prevent%20or%20respond%20to

Hybrid Threats. *A Strategic Communications Perspective*, NATO StratCom, COE, https://stratcomcoe.org/cuploads/pfiles/2nd_book_short_digi_pdf.pdf

Leigh Raymond et al, Information war and fight for truth, in *Western Balkans,* (2022): 3–5, https://www.cep.si/wp-ontent/uploads/2022/07/Fight-for-Truth.pdf

Kalenský, Jakub et al., *Amplify divisions, take advantage of vulnerabilities: Russian disinformation strategy Media'*, 25 November, 2021, https://euvsdisinfo.eu/greasing-the-wheels-with-disinformation/

Mînzărari, Dumitru (2021), A Hybrid War Early Warning Model: Towards an Early Warning Mechanism for the Republic of Moldova, Institute for European Policies and Reforms (IPRE), https://ipre.md/wp-content/uploads/2021/03/Paper_HW-EW-Model_30.03.2021_EN_final.pdf

Oliveira, Luciana et al., 'Using Social Media Categorical Reactions as a Gateway to Identify Hate Speech in

Patryk Pawlak, Understanding hybrid threats, June 24, 2015, https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/

Project of the National Security Strategy of the Republic of Moldova, Chişinău, 2023, https://presedinte.md/app/webroot/proiecte/Proiect_%20Strategie_11.10.23.pdf

Război hibrid şi atacuri cibernetice, (2017a), in: Revista Intelligence, 17 iulie 2017, https://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/

Războiul hibrid. Perspectiva conceptuală rusă (2017b), in: Revista Intelligence, 18 decembrie 2017, https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa/

Starea de securitate şi ameninţările hibride în adresa R. Moldova vor fi discutate la München, 4 martie 2023, https://zugo.md/toate-stirile/starea-de-securitate-si-amenintarile-hibride-in-adresa-r-moldova-vor-fi-discutate-la-munchen/214920/toate-stirile

Sterpu, Vladimir (2021) *Politica naţională de securitate a Republicii Moldova în contextul ameninţărilor şi războaielor hibride*. Studiu de politică publică, Chişinău.

Putină Natalia, Republica Moldova în contextul provocărilor şi riscurilor în domeniul securităţii informaţionale, în *Modernizarea guvernării din Republica Moldova: aspecte teoretico-aplicative*, Chiinău 2022, p. 134-143

Wardle, Claire, Derakhshan, Hossein (2017) *Information Disorder: Toward an interdisciplinary framework for research and policymaking*, Report Council of Europe, October, 2017. www.coe.int , https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/

Voicu, Marin, *Matriosca mincinosilor. Fake News, manipulare, populism*, Humanitas, 2018