No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-20

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Hybrid – defining the concept of the 21st century warfare, operations and threats

Cpt. Georgiana-Daniela LUPULESCU, Ph.D. Candidate*

*Ministry of National Defence, Bucharest, Romania
e-mail: geo.lupulescu@yahoo.co.uk

Abstract

Hybrid threats, as well as hybrid war, have become our century's constant, receiving numerous definitions over time, which clarify to a greater or lesser extent these concepts characterized mainly by ambiguity both in terms of means, as well as the forces involved or the geographical area of combat. It can be deemed at least as derisive to try to define a concept that arose from the need to include everything that is known in terms of techniques, means, methods and tools, but also what will appear in the not-too-distant future, thanks to the rapid technological evolution, used by state actors and non-states in an attempt to achieve their most diverse goals, be they military, political, social or even economic. This paper aims to provide a brief overview of the relevant literature on hybrid threats, operations and warfare, starting from the first attempt to define them and up to new attributes added in the meantime. We will analyze the characteristics, types, actors involved, and objectives pursued by them, resulting from the combination of several techniques, methods or tools.

Keywords:
hybrid threats; hybrid warfare; psychological operations; cyber; terrorism; disinformation.

The end o Hybrid threats have become a constant of the 21st century, being present in most of the conflicts of recent years and manifesting at the same time in periods of apparent peace. The need to study and adapt both legislation and practice regarding the emergence of these new types of threats was first stated in the US National Defense Strategy in 2005 (Department of Defense 2005). The new challenges that the United States was facing at the time, which became even more apparent after the terrorist attacks of September 11, 2001, increased this need for defense rethinking and reorganization. As a result, military analysts have focused their efforts on theorizing, but also finding patterns to define, understand, and counter hybrid threats.

The present article aims, first of all, to clarify the concepts of hybrid threat, hybrid operation, hybrid conflict, hybrid campaign, and hybrid war, as well as to analyze the characteristics, types, actors involved and the objectives pursued by them, resulting from the combination of several techniques, methods or tools, generated by the in-depth study of the literature in the field, with the aim of increasing awareness and understanding of the concepts.

The concept of hybrid threat is very closely related to hybrid warfare, as they are tools used before, during and after the completion of the conflict. At the same time, some authors believe that the purpose of a hybrid threat is to exploit vulnerabilities without declaring war (Solik, Graf and Baar 2022).

At the same time, the concepts of hybrid operation, hybrid conflict or hybrid campaign differ not only from the perspective of unfolding over time but also from the awareness of the situation in which they are found by all the actors involved. In this sense, the hybrid operation may involve the use of a limited number of tools and for a shorter period of time, while, from a conceptual point of view, the hybrid campaign tends to be carried out for a longer time and involves a series of threats of hybrid type pursuing a well-defined goal. On the other hand, both concepts, both conflict and war, describe the situation in which the parties fail to resolve their differences amicably, using diplomatic instruments or with the support of the international community. The difference between the two concepts may also lie in their legal framework. Categorizing a conflict as a war grants certain rights to the warring parties and obliges them to comply with international regulations.

The concept of hybrid warfare was originally used to describe the actions of non-state actors and their ability to use both increasingly sophisticated military means and non-military instruments (Reichborn-Kjennerud and Cullen 2016), being later attributed to state actors as well, due to their use of hybrid threats. The US National Defense Strategy foresees the existence of four types of capabilities and methods: traditional, asymmetric, catastrophic and disruptive, as well as the fact that they overlap and that actors are expected to use two or more such methods simultaneously, as was the case in the wars in Iraq and Afghanistan where insurgents

represented both a traditional force and an asymmetric challenge (Department of Defense 2005). Frank Hoffman also argues that in the future it is expected that there will be separate combinations or hybrid threats targeting the United States' vulnerabilities and that actors will likely use all modes of combat, perhaps even simultaneously (Hoffman 2007).

Hybrid warfare began to be looked at with particular attention only after Israel's war in Lebanon against Hezbollah in 2006, when Israel faced a force of well-trained and equipped insurgents capable of conventional warfare but who acted using techniques and unconventional tools (Schnaufer 2017, 17-31). The war between Israel and Hezbollah was also addressed by Hoffman who considers it "the prototype of the modern hybrid war" (Hoffman 2007). In this first hybrid war, we, therefore, find the characteristics of this type of conflict, as it was predicted by the US National Defense Strategy (Department of Defense 2005) and defined for the first time by Hoffman (Hoffman 2007). The non-linear character of this type of war, as well as the involvement of non-state actors that combine the conventional way of fighting with capabilities from the asymmetric spectrum, are the defining elements of the war between Israel and Hezbollah.

With the annexation of Crimea by the Russian Federation in 2014, the phenomenon of "hybrid war" began to gain momentum, so it was no longer treated as a theoretical notion, but became a term used to describe the state of insecurity and challenges in the security address of Western states while continuing to be a topic of interest among theorists who focused their efforts, especially on hybrid threats from the Russian Federation. States have begun to include the concept in their own security policy, thus recognizing the importance and reality of the existence of hybrid threats and hybrid wars and creating the legislative framework for taking defensive measures against them. Some examples of this would be The National Military Strategy of the United States of America (2015), The National Defense Strategy of the country for the period 2015-2019 (2015), The National Defense Strategy of the country for the period 2020-2024 (2020), The National Strategy for Countering Hybrid Interference of the Czech Republic (2021), The National Security Strategy of the Republic of Poland (2020). Moreover, the 2015 United States National Military Strategy states that "such hybrid conflicts may consist of military forces assuming a non-state identity, as Russia did in Crimea, or may involve an extremist organization that has rudimentary combined arms capabilities, as demonstrated by the Islamic State in Iraq and Syria. Hybrid conflicts also may be comprised of state and non-state actors working together towards shared objectives, employing a wide range of weapons, as we have witnessed in eastern Ukraine" (Dempsey 2015) thus identifying and exemplifying the materialization of hybrid conflict characteristics.

The existence of hybrid threats and the need to counter them in a unified and effective way represent one of the main objectives of both Western states and NATO or the European Union. The latter defines threats and hybrid campaigns

as "multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic and technological) to destabilize the adversary. They are designed to be difficult to detect or attribute and can be used by both state and non-state actors" (European Commission 2018). Furthermore, at the NATO level, within the latest Strategic Concept, issued in 2022, reference is also made to the Alliance's support of its members and partners, as well as to the coordination of actions to combat hybrid threats with other relevant actors, such as the European Union (NATO 2022).

Threat, operation, conflict or hybrid war?

The alternative use of the terms threat, operation, conflict or war, to which is added the quality of hybridity, can create confusion, both among theorists and decision-makers. We believe that one of the causes of this fact is the ambiguous character of hybrid operations, as:

- there is no clearly delimited space for fighting, a war zone, but, especially due to the informational tools used, the conflict often exceeds state borders;
- the actors involved, whether they are state or non-state are not always known, such as the situation where a state actor sponsors a non-state actor acting in favor of the former;
- the existence of a very fine line between war and peace, that gray area, which Jan Almäng talks about extensively (Almäng 2019);
- targeting a state's vulnerabilities using hybrid tools and methods is a constant state of international geopolitics, with such actions not being categorized as acts of war. An example of this would be the Russian Federation's use of propaganda and disinformation (Veebel 2016, 14-19);
- the threat involves a hypothetical, potential situation, which is what distinguishes it mainly from any form of ongoing event.

Consequently, for the clarity of the terms, although sometimes they are categorized as hybrid conflicts and sometimes as hybrid wars, we will use the term hybrid war to name a declared conflict between two or more state or non-state actors, which use both conventional and unconventional means in order to achieve strategic objectives. Jan Almäng claims that "if a conflict qualifies as a war, the participants in the conflict acquire rights and duties that they did not have before" (Almäng 2019), which does not always serve the interests and objectives of the combatant forces, which is why the purpose of using hybrid threats and tools becomes even to generate a situation in which it is unclear whether or not a state of war exists, and if it does, who is and who is not a combatant (Thornton 2015, 40-48). Avoiding the use of the term war led to the more frequent use of other terms, such as: conflict, operation, action, campaign, etc. hybrids, all having more or less the same characteristics. The difference may lie in the scale of the action, if the combatant forces know each other, or if there are only attacks of any kind by an unknown actor, etc.

The threat to a state's security can be seen as a combination of capability, intent and opportunity. The hybrid character in this situation results from the type of tools used. If, for example, an actor has the technical and intellectual capacity to conduct a cyber-attack, has the intention to do so, most likely due to the need to achieve certain strategic objectives, and the opportunity to execute the attack also arises, most often generated by the identification of a vulnerability, then the possibility of that actor executing a cyber-attack becomes a threat to those who have vulnerabilities in that domain and are in that actor's area of interest. To illustrate, we recall the cyber-attacks led by the Russian Federation on Georgia in 2008, which began a few months before the outbreak of the conflict later considered "the first war to take place in air, sea, land and cyberspace" (Mihai 2022). In the mentioned example, we identify the ability of the Russian Federation to use hackers to carry out cyber-attacks (they were attributed to the Russian Federation only in 2020 (Roguski 2020), the intention, demonstrated by the coordination of cyber-attacks with the use of conventional forces and the political situation in Georgia at the time, which did not serve the interests of the Russian Federation ("The newly elected president, Mikheil Saakashvili, engaged in close proximity to Western structures and attempted to reintegrate the provinces of South Ossetia and Abkhazia." (Mihai 2022), and last but not least, the opportunity generated by the vulnerability of Georgian IT systems.

Probably one of the most common questions among researchers and decision-makers in the last decade was "What is hybrid war?". Numerous scientific works have addressed this theme in an attempt to define and state a series of specific characteristics of this type of conflict. Among the first to stand out and make an essential contribution is Frank Hoffman, he is the one who named the conflicts characterized by the simultaneous use of tools from several fields: military, IT, psychological, economic, and political, by well-trained and flexible forces. In his view, hybrid warfare involves a number of different ways of waging a war that includes conventional capabilities, but also techniques and tools specific to asymmetric warfare, terrorist acts, indiscriminate violence, coercion, and even criminal actions (Hoffman 2007). At the same time, Thornton claims that one of the main characteristics of hybrid warfare is that "modes of conflict overlap and merge. Thus, the battlespace, as it is, can be shaped at one level by conventional operations and irregular activities and concurrently, at a higher level, by the application of underlying political and economic pressures" (Thornton 2015, 40-48). We can thus deduce that hybrid warfare involves the combined use of conventional means, military forces, and instruments, with asymmetric means. On the other hand, from the definition of hybrid war, given by Giannopoulos, Smith and Theocharidou (2021, 11), namely "the deliberate combination and synchronization of actions, by a hostile actor, specifically targeting systemic vulnerabilities in democratic societies", we can extract one of the specific characteristics of hybrid warfare, the targeting of vulnerabilities. So, we are no longer just talking about attacks directed at opposing military forces, but also about identifying and exploiting the adversary's vulnerabilities, including the civilian, non-combatant population. Also, the types

of actions used, and the threats launched against the enemy forces or the civilian population are very varied, from ballistic missile attacks, to psychological operations or cyber-attacks, usually used simultaneously on various targets, to achieve strategic objectives. At the same time, hybrid war has a strong ambiguous character, both in terms of understanding and using the concept itself (Janičatova and Mlejnková 2021), hence the many definitions, more or less overlapping, as well as the creation of policies and taking concrete actions to prevent or combat hybrid risks or threats.

Another big question mark about hybrid warfare and threats is whether they are new or just another way of naming what was already known. There are voices that say hybrid wars are as old as war itself (Galeotti 2016, 282-301), but also that while they are not new, they are different (Hoffman 2009b). At the same time, Giannopoulos et. al. (2021) consider that the evolution of war towards this hybrid form is mainly given by the dynamics of the security environment, by new tools, concepts and technologies, used simultaneously to exploit vulnerabilities. Hybrid warfare is therefore a relatively new concept, but one that encompasses the novelty generated by technology and its use for hostile purposes. At the same time, although the concept was introduced and developed more than fifteen years ago with the issuance of the US National Defense Strategy in 2005, when they first identified the need to adapt legislation, policies and defensive measures against these types of threats, only after the invasion of Crimea in 2014 did the concept of "hybrid war" gain special importance among theorists and decision-makers. Thus, both NATO and the European Union started including the term "hybrid" in their own policies and strategies (Mikac 2022).

Another characteristic that we consider defining in terms of categorizing the conflict as a hybrid one is represented by the blurring of the states' borders and the lack of clarity in determining the period of the conflict. What we intend to highlight is the fact that the tools used in a hybrid conflict, whether we are talking about cyber-attacks, propaganda, disinformation or terrorist attacks, do not necessarily surface in times of conflict, in the framework of a declared war, but can constitute hybrid threats to the security of states, which furthers the discussion of whether it is really a hybrid war or just a natural competition between states (Wither 2016, 73-87).

Types of Hybrid Threats

Giannopoulos et al. (2021) developed a conceptual model of hybrid threats in terms of actors, tools, affected domains, activity and target, where the latter was established as undermining decision-making capability. The tools used are not necessarily illegal or hybrid actions. For example, from the extensive list of hybrid threats, provided by Giannopoulos et. al. (2021), military exercises or the support of some political actors are neither illegal activities, nor do they constitute stand-alone hybrid threats. Instead, certain combinations of such instruments, used simultaneously and aimed

at destabilizing society from a political, economic, social or military point of view, are part of the category of hybrid threats.

As with other issues related to wars and hybrid threats, when it comes to identifying the types of hybrid threats, the situation is far from clear. The hybrid character is given by a number of factors, if only one person shares a piece of fake news on a social network, we cannot speak of the existence of a hybrid threat. One always takes into account the actors involved, the combination of kinetic and non-kinetic means, the purpose of the threat, the strategic interests and objectives, and of course the presence of ambiguity in all the mentioned aspects, to be able to say that a war or a hybrid operation is taking place.

The rapid evolution of technology has led to the emergence of innovative types of threats that have long gone beyond the strictly military sphere. Although some of them have existed for a very long time, such as psychological operations, of which we mention propaganda and disinformation, the way in which they are used, the extent to which they are carried out and the characteristic subtlety pose great problems in identifying, preventing and combating these hybrid threats. Treyger et al. (2022) for example, points out that the information war waged by the Russian Federation threatens to erode belief in factual truths and cause concrete damage through disinformation.

At the same time, cyber-attacks occupy a place of honor in the types of tools used in a hybrid war, sometimes even being the main "fighting" tool. For example, Russia is known to use such tactics through state-funded hacker groups and examples are multiple, from the cyber-attacks against Estonia in 2007, to those against Georgia in 2008 or those against Ukraine, both in 2014 with the annexation of Crimea (Mihai 2022) as well as those associated with the current conflict (Smith 2022).

State and non-state actors using hybrid threats

When we talk about hybrid war or hybrid threats, an important part of the discussion is to focus on the types of actors involved, the connections between them and the specific characteristics of each one. First of all, actors fall into two broad categories: state actors and non-state actors.

Whether we are talking about state actors or non-state actors, the discussion cannot be in terms of black and white, since, as in the case of the types of actions used, borders, objectives, the line of demarcation between the two categories it is blurred, unclear. If we take as an example the Israeli war in Lebanon, mentioned earlier in the article, the fusion between a non-state actor – Hezbollah and a state actor – Lebanon is at least obvious. As Hoffman suggests, "Hezbollah [...] has demonstrated a range of military capabilities similar to those used by states, including thousands of short-

and medium-range rockets and projectiles. This case demonstrates the ability of non-state actors to study and deconstruct the vulnerabilities of Western-style armies" (Hoffman 2007, 35-36). At the same time, Hezbollah benefited from weapons and training from Lebanon, a fact that unequivocally demonstrates the fusion of non-state - state actor.

On the other hand, Janne Jokinen and Magnus Normark believe that the use of non-state actors by states has always occurred, but the power of non-state actors has increased with the development of technology and financial services, areas in which certain non-state actors became experts over time. Consequently, the likelihood of their being used by states has increased considerably. At the same time, non-state actors can also find themselves in the position of adversaries of states (Jokinen and Normark 2022).

Another aspect to be considered is the fact that regardless of the form in which a non-state actor presents itself, whether we are talking about individuals, more or less legally constituted organizations, armed groups, etc., there are still no international laws that state the regime, role or responsibilities of non-state actors in an unequivocal manner (Kleckowska 2020). So, both states and non-state actors take advantage of this situation, the former by using non-state actors to achieve their goals, sometimes in dubious circumstances, and the non-states by having on the one hand the freedom to collaborate or not with the states and, on the other hand, by being able to exert influence on the policies of the states.

Vladimir Rauta suggests a classification of non-state actors that constitute combat groups, taking into account the relationship between them and states, into proxy, auxiliary, surrogate and affiliated forces thus:

- proxy forces are armed groups; they are not part of the regular forces but fight for them or on their behalf;
- auxiliaries are not part of the regular forces, but collaborate with them, being incorporated into the structure of the forces;
- the surrogates are used by the regular forces to complement their forces or even to replace them completely;
- affiliates are those that fight for regular forces, remaining officially out of the conflict (Rauta 2019).

Such a classification results from the way states use non-state actors, their involvement and the manner in which it takes place. Certain things in reality are not so clear since hybrid warfare and the actors using hybrid threats are characterized by ambiguity and the involvement of non-state actors is not always visible, which makes it difficult, if not impossible, to identify and catalog all the actors involved.

Non-state actors can either support the state for various reasons, have common goals, share the same ideology, etc., or it is the states that support, as sponsors, certain

groups or organizations for the same reasons, in which case the official combatant is the non-state actor and the state is not officially involved in the conflict. Non-state actors can take the form of any combination of insurgent or terrorist networks, organized crime groups, social groups such as clans, tribes, or ethnic groups, or ideologically or religiously motivated organizations, all of which may or may not be overtly or covertly supported by to legitimate states or businesses (Giannopoulos, Smith and Theocharidou 2021). The large number of types of non-state actors, their capabilities that sometimes reach or even exceed those of the state do not make the work of those fighting against hybrid threats any easier.

Regarding the actors involved in hybrid operations, the biggest challenge in trying to prevent or counter a hybrid threat is primarily their identification (Jokinen and Normark 2022), as there are situations where one cannot establish with accuracy the involvement of a particular actor. States can benefit from this situation, in the sense that they can always deny and refute any accusation of involvement in hybrid activities and, according to Giannopoulos et. al. "states directing activities through non-state entities exploit the opportunity to carry out activities of a harmful nature against other countries covertly. This has the advantage of making it more difficult for targeted states to detect activity related to the harmful state and respond before it occurs, but also to hinder the ability of the targeted state to attribute the harmful operation to the foreign state behind the event or series of events" (Giannopoulos, Smith and Theocharidou 2021).

Goals, objectives and targets

Like any conflict that has taken or will take place, hybrid wars are also based on a goal, a motivation, some objectives. Most of the time they fall into the political sphere by influencing the policies of some states, decreasing the trust of the population in state institutions, in a word weakening the government of a state or even its collapse. At the same time, any vulnerability of the state can be exploited within a hybrid operation, this being the mode of action of hybrid threats, identifying and exploiting the vulnerabilities of a state or of the way of fighting (Hoffman 2007).

Before launching a hybrid operation, after establishing the objectives pursued, the next step is the target selection. This action is closely related to the identification of vulnerabilities to be exploited. According to Cederberg and Eronen, they include all military capabilities, internal security, the internal and external political area, the economy, infrastructure, the standard of living and the resilience of the population to psychological operations (Cederberg and Eronen 2015). The hybrid operation takes place at the intersection of the identified vulnerability, the attacker's ability to exploit this vulnerability and the objectives pursued by the latter. Cederberg and Eronen argue that "hybrid operations are based on using identified asymmetries to make operations successful by confronting one's own strengths against the known

weaknesses of targets" (Cederberg and Eronen 2015). In his article, Cîrdei also claims that the mode of action in hybrid operations is based on exploiting vulnerabilities but also avoiding direct confrontation (Cîrdei 2016, 113-119). At the same time, recent history proves to us that certain objectives still cannot be achieved without an active military component as is the case in the current Russian-Ukrainian conflict, which includes everything from armed aggression to cyber-attacks (Viasat 2022) or psychological operations (EU vs DiSiNFO 2022).

A particular reason why states would engage in hybrid actions, especially through non-state actors with certain capabilities, could be to gain access to certain infrastructures or systems. Such a situation is presented by Giannopoulos et. al. This is Airiston Helmi, a real estate company in Finland that could have been used as a cover to make important strategic investments and prepare the properties for later use. In this situation, Russian citizens would have bought very well secured properties, with exceptional technical equipment to accommodate a large number of people and located in an important strategic area of Finland. The author considers this a very good example of "how foreign states can act through third parties to influence, intervene or obstruct the affairs of states to generate negative consequences or to establish the ability to do so when desired" (Giannopoulos, Smith and Theocharidou 2021).

Conclusions

The hybrid attribute added to threats to the security of states and the wars waged in recent years has created polemics and differences of opinion both in the academic world and at political level. Hybrid wars and their complexity have been and will probably be studied for a long time to come especially because the information dimension, which often underlies the manifestation of many other types of threats, is in continuous development.

Although at the level of theorists there is no consensus regarding the use of the terms threat, conflict, operation or hybrid war, we can state that the tools used and the ways of combining them, the involvement of both non-state and state actors, the goals pursued and, perhaps most importantly, the ambiguity of all the above-mentioned aspects, are defining elements and actually the mark of the hybrid character of any threat, operation, any conflict or war.

The emergence and evolution of the concepts of threats and hybrid wars are not new. The hybridity of conflicts and threats does not create an entirely new concept, but one in a dynamic continuum, adapted to the technological capabilities of our times. Although the term "hybrid" entered the vocabulary of academics and political-military decision-makers almost 20 years ago, but more significantly after 2014, this way of fighting can also be observed in much older conflicts, especially when

we refer to the use of non-military tools such as propaganda or disinformation. Moreover, the hybrid character attributed to contemporary threats and conflicts began to be increasingly associated with their cyber dimension. The latter is a tool in itself but also a means of implementing other types of threats, which generates not only ambiguity but also the blurring of state borders, actions often taking place in cyberspace. Security and defense against hybrid warfare and threats have been and will continue to be a challenge, especially due to the inherent ambiguity, both in terms of the tools used, their combination and synchronization, and in terms of identifying the actors involved.

The evolution and dynamic character of the concepts of hybrid warfare and hybrid threat represent a challenge for the security of Western states. Their defining characteristics no longer allow either individual defense or treating each threat separately, but a joint approach of states, rigorous defense planning including all key areas of society will be required. Furthermore, identifying and mitigating society's vulnerabilities before they are exploited by hostile entities should be one of the main goals of states.

References

Administrația Prezidențială. 2015. "Strategia Națională de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf.

—. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020-2024."

Almäng, Jan. 2019. "War, vagueness and hybrid war." *Defence Studies* 19 (2): 189-204.

Cederberg, Aapo și Pasi Eronen. 2015. "How can Societies be Defended against Hybrid Threats." *Geneva Centre for Security Policy* (9).

Cîrdei, Ionuț Alin. 2016. "Countering the hybrid threats." *Revista Academiei Forțelor Terestre* (2): 113-119.

Dempsey, Martin. 2015. "The National Military Strategy of the United States of America." https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

Department of Defense. 2005. "National Defense Strategy of the United States." https://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=tFA4Qqo94ZB0x_S6uL0QEg%3d%3d.

EU vs DiSiNFO. 2022. "Key Narratives in Pro-Kremlin Disinformation: «Nazis»." https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation-nazis/#.

European Commission. 2018. „Comunicare comună către Parlamentul European, Consiliul European și Consiliu." https://data.consilium.europa.eu/doc/document/ST-10242-2018-INIT/ro/pdf.

Galeotti, Mark. 2016. "Hybrid, ambiguous, and non-linear? How new is Russia's new way of war?" *Small Wars & Insurgencies* 27 (2): 282-301.

Giannopoulos, Georgios, Hanna Smith și Marianthi Theocharidou. 2021. *The lanscape of hybrid threats: A conceptual model.* Luxembourg: Publications Office of the European Union.

Hoffman, Frank. 2007. *Conflict in the 21st century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

—. 2009a. "Further Thoughts on Hybrid Threats." *Small Wars Journal.*

—. 2009b. "Hybrid Warfare and Challenges." *JFQ* (52): 34-48.

Janičatova, Silvie și Petra Mlejnková. 2021. "The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities." *Contemporary Security Policy.*

Jokinen, Janne și Magnus Normark. 2022. "Hybrid threats from non-state actors: A taxonomy." *Hybrid CoE Research Report.*

Kleckowska, Agata. 2020. "States vs. non-state actors – a public international law perspective." *Hybrid CoE Strategic Analysis.*

Mihai, Paul. 2022. „Provocări hibride de natură cibernetică." *Infosfera* (2).

Mikac, Robert. 2022. "Determination and Development of Definitions and Concepts of Hybrid Threats and Hybrid Wars: Comparison of Solutions at the Level of the European Union, NATO and Croatia." *Politics in Central Europe* 18 (3): 355-374.

Ministry of Defense Czech Republic. 2021. "The National Strategy for Countering Hybrid Interference of Czech Republic." https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf.

NATO. 2022. "NATO 2022 Strategic Concept." https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

President of the Council of Ministers. 2020. "The National Security Strategy of the Republic of Poland." https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

Rauta, Vladimir. 2019. "Towards a typology of non-state actors in „Hybrid Warfare": Proxy, auxiliary, surrogate and affiliated forces." *Cambridge Review of International Affairs.*

Reichborn-Kjennerud, Erik și Patrick Cullen. 2016. "What is Hybrid Warfare?" *Policy Brief* (Norwegian Institute of International Affairs) (1).

Roguski, Przemyslaw. 2020. "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace." https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Schnaufer, Tad A. 2017. "Redefining Hybrid Warfare: Russia's Non-linear War against the West." *Journal of Strategic Security* 10 (1): 17-31.

Smith, Brad. 2022. "Defending Ukraine: Early Lessons from the Cyber War." https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Solik, Martin, Jan Graf și Vladimir Baar. 2022. "Hybrid Threats in the Western Balkans: A Case Study of Bosnia and Herzegovina." *Romanian Journal of European Affairs* 22 (1).

Tenenbaum, Elie. 2015. "Hybrid Warfare in the Strategic Spectrum an Historical Assessment." In *NATO's response to hybrid threats*, by Guillaume Lasconjarias and Jeffrey A. Larsen, 95-112. Rome: NDC Forum Paper.

Thornton, Rod. 2015. "The Changing Nature of Modern Warfare." *The RUSI Journal* 160 (4): 40-48.

Treyger, Elina, Joe Cheravitch și Raphael S. Cohen. 2022. *Russian disinformation efforts on social media.* Santa Monica: RAND Corporation.

Veebel, Viljar. 2016. "Estonia confronts propaganda: Russia manipulates media in pursuit of psychological warfare." *Per Concordiam* 7 (1): 14-19.

Viasat. 2022. "KA-SAT Network cyber attack overview." https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Wither, James K. 2016. "Making Sense of Hybrid Warfare." *Connections: The Quarterly Journal* 15 (2): 73-87.