CONCEPTUALISATION, OPERATIONALISATION AND CONNECTION BETWEEN "HYBRID THREATS" AND "SECURITY CULTURE"

Colonel Prof Adrian LESENCIUC, PhD

"Mihai Viteazul" National Intelligence Academy

Corneliu Mugurel COZMANCIUC, PhD Candidate

"Mihai Viteazul" National Intelligence Academy

To date, the potential for addressing hybrid threats through a strong security culture remains underdeveloped, while the nation-wide responses are still lacking clarity and comprehensiveness.

The present paper presents the link between a wide range of emerging threats that are currently challenging countries and institutions and the potential of mitigating such issues through security culture while building and consolidating a resilient national system. Continuously under the threshold of formally declaring warfare, hybrid threats have been demonstrating the futility of responses implicating only institutions with responsibilities in the fields of security and defence.

Subsequently, we argue that cultivating measures, procedures and good practices for boosting security culture through a whole-of-government approach would ensure a useful framework for tackling such challenges, while also aiming for a joint civilian-military response. The hybrid toolbox needs to be pre-empted by active and passive measures, the ability of societies and institutions to bounce back from shocks being sustained by both resilience and robust measures that would enhance civil and military preparedness.

By assessing the rise of hybrid threats and their position in the Russian strategic thinking and comparing the Western doctrines mirroring these challenges, we obtain an overview on the differences in concept and operations that are currently lacking clarity.

Considering that national vulnerabilities have now global implications, sovereign action must be effectively completed by alliances and partnerships, while also keeping in mind the made-to-measure hybrid actions with specific and narrow targets. Through examining the components of hybrid and information warfare, we stress the fact that it is high time to have and use a unified vocabulary in support of building a common security culture, necessary for this ever-changing security landscape.

Keywords: hybrid threats; hybrid warfare; information warfare; security culture; national resilience;

INTRODUCTION

The emergence of confrontations in the online environment brings us to a new form of war. A war in which soldiers no longer face each other, but individuals with technical skills in IT domain become attackers and the civilian population becomes the target – the asymmetric warfare. It is defined as *"unconventional strategies and tactics adopted by a participant in a conflict when the capabilities of the belligerent powers are not simply unequal but are significantly different so that they cannot carry out similar attacks on each other"* (Sexton, 2014).

Participants become both state and non-state political actors (individuals or organisations that have significant political influence but are not particularly allies of a state).

The thinking behind this type of confrontation has stemmed from the use of guerrilla tactics in the online environment: neutralising the technical-tactical advantage of the opponent, neutralizing the support of the population for military forces, traditional allies or even the government of the target state.

One of the peculiarities of asymmetric warfare is the use of *soft* and *hard* powers in the same confrontations. If hard power represents the use of force or the coercive capacity of a state, *soft* power means the co-optation of others in the efforts of a state (Nye, 2004, p. 5). The difference between the two forms of power is described as it follows: *"**hard** power requires compliance-based mainly on tangible power, while **soft** power cultivates compliance through a variety of policies, qualities and actions, indirectly and through non-coercive measures"* (Gallarotti, 2011, pp. 10-11).

One of the peculiarities of asymmetric warfare is the use of soft and hard powers in the same confrontations. If hard power represents the use of force or the coercive capacity of a state, soft power means the co-optation of others in the efforts of a state.

The integrated use of these facets of the concept of power has been called *smart* power. It is seen as *"an approach that emphasises the need for a strong military presence, but which invests heavily in alliances, partnerships and institutions at all levels, to extend one's influence and legitimize one's actions"* (Armitage, 2007, p. 7).

GERASIMOV DOCTRINE

Russian General Valery Gerasimov's article, *"The value of science is in perspective: new challenges call for a rethinking of forms and methods of conducting combat operations"* brings *"hybrid threats"* among the major concerns of the Western world and is interpreted as proposing a new Russian approach to a confrontation which combines conventional and unconventional warfare with aspects of national power, often referred to as *"hybrid warfare"*.

The US government defines unconventional warfare as *"activities conducted to assist a resistance movement or insurgency in coercing, disrupting or overthrowing a government or occupying force, operating through or with the help of the underground, auxiliary or guerrilla forces in a forbidden area"*. (Public Law 114-92, 2015, Sec. 1097, (d)).

The US government defines unconventional warfare as "activities conducted to assist a resistance movement or insurgency in coercing, disrupting or overthrowing a government or occupying force, operating through or with the help of the underground, auxiliary or guerrilla forces in a forbidden area".

Other concepts used by Gerasimov were *"the new generation war"*, characterised by the erosion of the demarcation lines between the state of war and the state of peace and *"non-linear war": "a means to reach desired strategic orientation and geopolitical outcomes primarily using non-military approaches"* (Morris, 2015).

Gerasimov came to these conclusions by researching how the West is waging war, relying less on traditional invasions such as Iraq in 2003 and more on the 2011 intervention in Libya, the events of the *Arab Spring* and the *"colour revolutions"*. In his view, the West was a pioneer in indirect approaches to war, using political subversion, propaganda and social networks, along with economic measures such as sanctions. Humanitarian interventions, the use of Western special forces, funding for *"democratic"* movements and the deployment of mercenaries were all features of an American doctrine of indirect war, emphasising that there is a four-to-one ratio between non-military and military measures in modern conflict, but he was talking about how the West shapes the battlefield before the intervention.

But Gerasimov was not the first to notice this. George F. Kennan put forward a similar argument in his 1948 memoir on the organisation of political warfare: *"Political warfare is the employment of all means at the command of the nation to achieve its national goals. ... They range from such abrupt actions as political alliances, economic measures and «white» propaganda to covert operations, such as the support of «friendly» foreign elements, «black» psychological warfare*

and even the encouragement of underground resistance in hostile states" (Kennan, 1948, pp. 1-2).

Three major theories have been identified, addressing the understanding of information warfare: the *"insurrectionary warfare"* proposed by Evgheni Messner, the *"net-centric warfare",* the vision of Aleksandr Dugin and the *"information warfare"*, developed by Igor Panarin.

Messner's vision of the international politico-military context was strongly influenced by the conflict between the great victories of World War II, Russia and the United States. He notes that after 1945, Trotsky's explanation of the Treaty of Brest-Litovsk – *"neither war nor peace"* – applies globally. He also interpreted the *"proxy wars"* during the Cold War as part of a more general picture. For these reasons, Messner foresaw the need for a new kind of war, given that the *"classic"* became impossible to fight.

Three major theories have been identified, addressing the understanding of information warfare: the "insurrectionary warfare" proposed by Evgheni Messner, the "net-centric warfare", the vision of Aleksandr Dugin and the "information warfare", developed by Igor Panarin.

One of the distinctive features of the insurrectionary warfare is the increasing importance of the psychological/informational dimension. The main purpose of the war became not to capture the physical territory of the enemy, but to conquer minds and hearts by weakening official narratives. The confusion and discomfort of the target population have become objective, and the main tools for doing so are propaganda and agitation.

Messner observes two main features of information warfare: *"propaganda by the word"* and *"propaganda by the deed"*. If the first includes the official discourse of the authorities and forms of cultural-artistic manifestations, the second includes successful deeds, achieved in a timely manner – *"an idea gains credibility when it is supported by military, political, social, diplomatic and economic achievements"*. So it is not only what is said, written, published, disseminated, but also what is done: *"In times of psychological warfare, neither victory in battle nor territorial gains are objective in themselves: their main value lies in their psychological effects".* Therefore, the need for congruence between word and deed: on the one hand, discourse must be seconded by concrete action; on the other hand, the actions must be brought to the public's attention through a tailor-made speech. (Freedman, 2017, p. 68 et seq.).

Propaganda *"should not be defensive, justifying; instead, it should actively stimulate the emotions and thoughts of our soldiers, combatants and non-combatants"* (Freedman, 2017, p. 68). Such actions will be doomed to failure if their discourse does not adapt to the context. A careful study of the cultural context and the national or regional specificities of the target populations can provide the answer to these problems. The concealment of propaganda is an essential condition: *"Both defensive and offensive propaganda is doomed to failure if it looks like propaganda"* (Fridman, 2017, p. 68).

Dugin and Panarin stand out by the fact that they were themselves participants in the information warfare, as opinion leaders. Panarin offers the basic tools of the information struggle, which he divides into secret and non-secret categories. These include propaganda, institutional intelligence, monitoring and analysis, organisational component (coordination and direction channels), secret agents with influence in the media, and other combined channels, including special forces of operations (sabotage operations carried out under foreign flag).

The other two Russian theorists, Dugin and Panarin, academics and mentors, stand out by the fact that they were themselves participants in the information warfare, as opinion leaders. Panarin offers the basic tools of the information struggle, which he divides into secret and non-secret categories. These include propaganda, institutional intelligence, monitoring and analysis, organisational component (coordination and direction channels), secret agents with influence in the media, and other combined channels, including special forces of operations (sabotage operations carried out under foreign flag). The stages of the information operations management process would be the following: (1) forecasting and planning, (2) organisation and stimulation, (3) feedback, (4) operation regulation, (5) performance monitoring.

Aleksandr Dugin proposes the term "*network-centric warfare":* which means the creation of a new military information infrastructure involving interactive elements and rapid means of communication. The *"Eurasian network"* would provide asymmetrical response to the *"net-centric challenge in the United State"*. The missions will be carried out by *"a special group of senior officials, the best mission-oriented staff of the Russian secret services, intellectuals, scientists, political scientists and the body of patriotic journalists and cultural activists must be created for this purpose"*. The model of the *"Eurasian network"*, as opposed to the *"Atlantic network"*, is expected to combine the basic elements of American postmodernism and the net-centric approach with the Russian reality.

This approach could be successful, provided that the Russian armed forces, secret services, political institutions, information and communication systems, etc. are *"postmodernised"*. An internet

warfare can only be won if the country uses network resources, and they must be adapted to Russia's reality and objectives and efficient technologies, according to Dugin's diagnosis.

The recent information warfare and network warfare of Russian origin should be seen as a product of traditional political technologies that have been used for years and represent the legacy of USSR. Contemporary Russian information geopolitics is based on the Soviet understanding of psychological warfare and reminiscent mental stereotypes. Propaganda remains the key tool of the information warfare. Its distinctive features are language (the language of emotions and prejudices but not facts), content (respect for official Kremlin propaganda) and function (discrediting the opponent). But we do not know whether the specifically Russian tools of information warfare will be effective in a possible ideological crusade against the West. Messages issued for this purpose are unbelievable and easy to verify in the age of new technologies. Moreover, the ideas offered are not attractive. However, if propaganda tends to fail in the West, ideological news based on misinformation finds fertile ground in the East.

There are several definitions of information warfare proposed by Whitehead, some of them accepted by the US military and some of the independent sources, the most complex and comprehensive being: Information warfare consists of "actions carried out in the information environment in order to prohibit, exploit, alter, destroy or ensure the viability of the information. The goal is to ensure the informational advantage".

THE INFORMATION WARFARE

The specific terminology of "*information warfare"* appeared in the early 1990s, but at least two distinct meanings can be distinguished in its understanding: a) disruptive measures for systems based on information flows and b) influencing perceptions by affecting the content of information, the first being oriented towards technical aspects, the second on knowledge (Freedman, 2019, p. 311).

There are several definitions of information warfare proposed by Whitehead, some of them accepted by the US military and some of the independent sources, the most complex and comprehensive being: Information warfare consists of *"actions carried out in the information environment in order to prohibit, exploit, alter, destroy or ensure the viability of the information. The goal is to ensure the informational advantage"*. (Whitehead, 1999, pp. 4-5).

This type of war has the following main characteristics; low costs, difficult to define traditional boundaries, increased role of perception management, a challenge for strategic information management, formidable problems for tactical warning and attack assessment,

difficulty in building and supporting coalitions, country vulnerability (Molander et al, pp. 15-16). According to these characteristics, the delimitations proposed by the traditional concept of war are becoming more and more difficult: Who is a combatant and who is not? Who attacks and when? Are armistices and the at least temporary cessation of hostile actions possible? Moreover, the consequences of non-state political actors' involvement in the conflict can have serious consequences for society as a whole: an affected private entity can lead to a loss of public confidence, unemployment and, ultimately, social unrest.

Information warfare can take more or less subtle forms. Internet access turns the civilian population into participants in this war, which is not only subject to propaganda shootings but it also, in some courts, becomes a vector for the dissemination of this information. If initially false information could be countered by truth and evidence, this method works much less in a social world populated by trolls and robots (Fukuyama, 2017).

In the information warfare, opponents are hidden and efforts to destroy their anonymity are often doomed to failure. An example of an information attack is Operation "Grizzly Steppe": the US intelligence community learned that GRU had access to the Democratic National Committee's IT resources from July 2015 to July 2016.

Fake news phenomena are exploited by media institutions purchased or financed in a non-transparent way. The rise of artificial intelligence technologies has made it possible to *use deep fakes,* video recordings in which a person's face is replaced with that of a political or social leader, the messages issued by them are altered or even *"built"* from pieces of speech arranged in such a way that they support positions which the presented leader would not have normally expressed. Propaganda is emotionally charged and is based on the aggressor's interest, to change the collective feeling towards the aggressor's intentions and goals (Nate, Rațiu, 2017, p. 2).

In the information warfare, opponents are hidden and efforts to destroy their anonymity are often doomed to failure. An example of an information attack is Operation *"Grizzly Steppe"*: the US intelligence community learned that GRU (Russia's main intelligence agency) had access to the Democratic National Committee's IT resources from July 2015 to July 2016. Russian intelligence services were able to extract large amounts of data from Democratic National Committee computers, then transmitted by *Guccifer 2.0* to Wikileaks.com and DCLeaks.com. The events were followed by a massive psychological

operation aimed at discrediting Hillary Clinton, a candidate in the US presidential election and, especially, eroding confidence in the institutions of the United States (Rugge, 2018, pp. 4-5).

SECURITY CULTURE, A TOOL TO FIGHT AGAINST THE INFORMATION WARFARE

Security culture is a model of basic assumptions, values, norms, rules, symbols and beliefs that influence the perception of challenges, opportunities and/or threats and how to feel and think about security, behaviour and activities of active social actors, individual or collective, connected in a variety of ways (Piwowarski, 2017, pp. 17-19).

Emerged in September 1977, the concept of *"security culture"* evolved from a limited understanding in the military or strategic field to its application throughout society. Kai Roer provides an inclusive definition of security culture: *"The ideas, habits, and social behaviours of an individual or group that help them be free from threats and dangers"* (Roer, 2015, p. 14) According to him, security culture consists of three fundamental elements: technologies, policies and competencies; technologies are tangible and intangible (mental models, standards and know-how) (Roer, 2015, p. 19).

Among the Romanian researchers, Lungu et al provide a definition that broadens the scope of the concept: *"Security culture is the result of social interactions that take place in groups, organizations, communities concerned with social security issues, learning processes and knowledge accumulation, in accordance with the human needs of protection, safety, shelter. The security culture is adaptive, develops in relation to the evolution of society and is transmitted between generations through various forms of written and oral communication, as well as through practices to support security values"* (Lungu, 2018).

The Security Culture Barometer, published in 2018, reveals that Romanians are rather interested in a conspiratorial side of the information they take from the news, caused by the lack of critical thinking in certain strata of society. This can intensify the fake news phenomena, which can reach as many people as possible (INSCOP, 2018, p. 44).

According to the same study, there are no significant differences between populations in urban and rural areas of residence, nor between different age groups, gender or depending on the historical

"Security culture is the result of social interactions that take place in groups, organizations, communities concerned with social security issues, learning processes and knowledge accumulation, in accordance with the human needs of protection, safety, shelter. The security culture is adaptive, develops in relation to the evolution of society and is transmitted between generations through various forms of written and oral communication, as well as through practices to support security values".

region in which they live, when it comes to social categories sensitive to conspiracy tendencies.

A study on the digital behaviour of Romanians, published in 2018, shows how they underestimate the power of false news and inaccurate information. Over 50% of respondents said that their opinions are to a small or medium degree influenced by inaccurate information, but the high rate of those who did not answer this question (18%) leads to the conclusion that the issue of how to trust the news modelling opinions and actions is not considered at all by many Romanians (Bârgăoanu, Radu, 2018).

Former CIA Director Michael V. Hayden said that Russia's involvement in the US presidential election was the political equivalent of the 9/11 terrorist attacks, an unprecedented vulnerability. Therefore, the State has the task to strengthen governance and response mechanisms at the institutional level, but also to build alliances with those who are subject to the same threats at the cultural, political and military levels.

The main and most effective methods of a counterattack are awareness and education. The responsibility for both lies with both the citizen and the state institutions. *"Cyber-hygiene"* will not protect the country from advanced and persistent attacks, hybrid scenarios or a state-of-the-art war, but it is an easy and relatively inexpensive way to allocate few financial and technological resources to deal with serious threats. By cultivating the critical spirit, a society will be able to build effective barriers against *fake news*, education reducing the echo chamber effect of social media (Rugge, 2018, pp. 6-7).

Adherence to the basic principles of democracy: decisional transparency, openness and the rule of law create a political environment in which the interference of foreign entities in democratic processes can be easily observed and countered. Instead, a climate of public hostility to the ideological opponents of political power will erode the legitimacy of democratic institutions.

Former CIA Director Michael V. Hayden said that Russia's involvement in the US presidential election was the political equivalent of the 9/11 terrorist attacks, an unprecedented vulnerability. Therefore, the State has the task to strengthen governance and response mechanisms at the institutional level, but also to build alliances with those who are subject to the same threats at the cultural, political and military levels. Partners will need to actively participate in establishing confidence-building measures as well as the rules of conduct of states in cyberspace (Ibid, p. 8).

Institutional efforts will be in vain without citizens having adequate tools to filter information. The information warfare exploits social cleavages, erodes citizens' trust in institutions, decision-makers,

international organisations, but also in the measures taken by them to ensure their security. The manipulation of information by hostile state and non-state actors can be countered by a solid security culture.

The *whole-of-society* approach accepts that security risks are a threat to society as a whole and any member can become a vulnerability in the absence of a security culture. State institutions can develop and promote a culture of security among citizens through transparency and awareness-raising. Citizens can develop mental hygiene skills by developing critical thinking and by accessing the information resources provided by the state.

At the programmatic level, in Romania, the term *"security culture"* appears in the *"Guide of the National Strategy for the defence of the country for the period 2015-2019"*, adopted by the Supreme Council of National Defence. According to it, security culture represents "the totality of values, norms, attitudes or actions that determine the understanding and assimilation at the level of society of the concept of security and its derivatives (national security, international security, collective security, insecurity, security policy, etc.) (Administrația Prezidențială, 2015, p. 7).

The Romanian state sees the security culture as a condition of social normalcy and the citizen in a double role: beneficiary and generator of security. The ways for the development of security culture are stimulating the public interest in security culture, placing security education courses in the formal education process, training programs accessible to the general public, identifying public experts as promoters of awareness programmes etc. (Ibid, p. 14).

The *"National Defence Strategy 2020-2024"* continues the vision of the previous document, adopted in 2015, but elaborates on some aspects and introduces complementary concepts to the security culture. According to the document, Romania must become *"a resilient state, able to adequately relate to the unpredictability and scale of developments in the security environment. This requires a strong state, a state that is aware of the need to develop its own rapid and efficient response mechanisms and, inherently, a solidly sized security culture – including among its citizens"* (Ibid, p. 6). But this desire to create a resilient state is interdependent with the level of security culture of its citizens (Ibid, p. 12).

The "National Defence Strategy 2020-2024" elaborates on some aspects and introduces complementary concepts to the security culture. According to the document, Romania must become "a resilient state, able to adequately relate to the unpredictability and scale of developments in the security environment. This requires a strong state, a state that is aware of the need to develop its own rapid and efficient response mechanisms and, inherently, a solidly sized security culture – including among its citizens".

The cited document places a major emphasis on the interdependence between the culture of security and resilience, but also on the creation of a *"culture of prevention, through the active and continuous preparation of the population to react to a major emergency"* (Ibid, p. 37). The effort to achieve them will be *"coordinated at the strategic level, based on a single implementation plan"*, horizontally, through the cooperation of institutions gathered in working groups.

CONCLUSIONS

Below the threshold of an official declaration of war, hybrid threats have demonstrated the futility of responses involving only institutions with responsibilities in the field of security and defence. The continuous state of *"siege"* requires the assumption of an alert conscience of the whole society, being essential the training, education and culture in fields that are no longer found in conventional trenches, but homes and institutions.

Following the effects of hybrid threats on state cohesion and societal security, this article emphasises the importance of citizen participation in state security through the development of a strong individual security culture.

Following the effects of hybrid threats on state cohesion and societal security, this article emphasises the importance of citizen participation in state security through the development of a strong individual security culture. It is based, first of all, on the promotion of the core values of democratic societies, represented by transparency, openness and consolidation of the rule of law, as well as on alliances between different categories or threatened entities, being able to be achieved both by practical methods and by solutions to make truthful information viral, which would lead to a general increase in the level of digital literacy.

BIBLIOGRAPHY:

1. Armitage, R.L. (2007). *How America Can Become a Smarter Power. CSIS Commission on Smart Power. A Smarter, More Secure America*. Washington, D.C.: Center for Strategic and International Studies.
2. Bârgăoanu, A., Radu, L. (2018, June). "*Fake News or Disinformation 2.0? Some Insights Into Romanians' Digital Behaviour".* In *Romanian Journal of European Affairs*. Vol. 18, nr. 1.
3. Freedman, L. (2019, November). *Viitorul războiului*. București: Kronika.
4. Fukuyama, F. (2017, 12 January). *The Emergence of a Post-Fact World, Project Syndicate*, https://www.project-syndicate.org/onpoint/the-

emergence-of-a-post-fact-world-by-francis-fukuyama-2017-01, retrieved on 13 May 2020.
5. Gallarotti, G.M. (2011). *"Soft Power: What It Is, Why It's Important, and the Conditions Under Which it Can Be Effectively Used"*. In *Journal of Political Power*. Middletown.
6. Kennan, George F. (1948, 30 April). *The Inauguration of Organized Political Warfare, Digital Archive, International History Declassified*. Washington D.C.: Wilson Center.
7. Lungu, C., Buluc R., Deac, I. (2018). *Promovarea culturii de securitate*. București: ProSCOP.
8. Molander, R.C., Riddile, A.S., Wilson, P.A. (1996). *Information Warfare. A New Face of War*. California, Santa Monica: RAND.
9. Morris, V.R. (2015). *Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrin*e. In Small Wars Journal, https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine, retrieved on 12 October 2020.
10. Nate, S., Rațiu, A. (2017). "*Defending the Truth and Counter Information Warfare".* In *Europe. Knowledge-Based Organization*. Vol. XXIII, no. 1.
11. Nye Jr., J.S. (2004). *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.
12. Piwowarski, J. (2017). "*Three Pillars of Security Culture, Security Dimensions".* In International & National Studies, nr. 22.
13. Roer, K. (2015). *Build a Security Culture*. Cambridgeshire: IT Governance Publishing.
14. Rugge, F. (2018, January). *"Mind Hacking: Information Warfare in the Cyber Age"*. In *Instituto Per GliStudi Di Politica Internazionale*.
15. Sexton, E. (2016). *Asymmetrical Warfare*, https://www.britannica.com/topic/asymmetrical-warfare, retrieved on 12 October 2020.
16. Whitehead, Y.G. (1999). *Information as a Weapon. Reality vs. Promises, Air University*. Alabama: Maxwell Air Force Base.
17. Administrația Prezidențială (2015). *Ghidul Strategiei naționale de apărare a țării pentru perioada 2015-2019*. București.
18. Administrația Prezidențială (2015). *Strategia națională de apărare a țării 2015-2019*. București.
19. Administrația Prezidențială (2020). *Strategia națională de apărare a țării 2020-2024*. București.
20. INSCOP (2018). *Barometrul culturii de securitate – februarie 2018*, https://larics.ro/wp-content/uploads/2018/04/Raport-sondaj-INSCOP-barometru-LARICS-partea-1.pdf, retrieved on 12 October 2020.