THE MODERN THREATS TO INTERNATIONAL SECURITY

Captain Ilie IFTIME, Ph.D Candidate*

Abstract: *This article highlights a comprehensive approach of modern threats to international security and also identifies how they adjust to new environments of action. Therefore, using the method of contextual analysis, I will answer the following research questions: What are the main challenges affecting the current security environment? Which of these represents the most widespread threat and involves possible prospects for the future? Thus, the aim of this approach is to provide, in the first part, an up-to-date examination of the transfiguration of the current security threats by observing the dominant trends, useful for future scientific research, and in the second part I will demonstrate, based on the views of some specialists in the field but also as a result of indirect observation on the developments of international conflicts, that hybrid war remains the defining concept for recent events in international security.*

Keywords*: threats, international security, globalization, grey zone, hybrid warfare, resilience.*

Introduction

The current security environment is characterized mainly by its dynamism, complexity and unpredictability, and "the challenges tend to become more and more diffuse, less predictable and multidimensional, constituting both an external feature of security and an internal one and, of course, becoming an indispensable component of security policies and strategies. For these reasons, the need for international cooperation has increased as a basis for ensuring the stability of the security environment, which must ensure a sense of confidence and peace, by guaranteeing the absence of any danger"[1]. Although the need for pro-active strategic communication is felt sharply, it must be understood that the slowing/fragmentation of this process is achieved due to the difficulties of analyzing large volumes of data and information. A phenomenon that arises, among other things, due to the need to increase the response time to different situations, which no longer correspond to the predictions and pre-calculated scenarios.

The communication and inaccurate, interpretable and concealed course of some important actors on the international stage is represented by

* "Carol I" National Defense University, Bucharest, Romania, E-mail: andreiaalbu1@gmail.com

[1] RICHICINSCHI Iurie, Riscuri și amenințări potențiale la adresa securității internaționale, 2016, p. 105, available at https://ibn.idsi.md/sites/default/files/imag_file/105_112_-Riscuri%20si%20amenintari%20potentiale%20la%20adresa%20securitatii%20internationale.pdf, accessed on 19.01. 2024

their desire to reconfigure/influence the balance of power. This objective is pursued by various means such as: nonlinear movements in international relations, resizing spheres of influence and participating in the "technological arms race"[2]. This last aspect is topical and is noted in the World Economic Forum's Global Risk Report 2023 and describes the major impact on the economy and consequently on the societal sector. The causality of the phenomenon is given by the fact that this race is counter-chronometer, it is based on the principle weapon-counter-weapon (some actors seeking to discover the new technologies first, that dominate the old ones and place them in advantage over the others) and consequently the interventions of the state in redirecting the economic sector are multiple.

The influence of the balance of power, which is "an organizing element of international relations between states", according to Hans Morgenthau[3], is closely linked to the threat balance equation that involves four components: power, proximity, offensive capacity and offensive intentions. Power cannot be a threat unless it is corroborated with the other components and in an era of globalization, where the space-time dimension is increasingly compressed, "the proximity factor is present in any type of identifiable threat"[4]. Furthermore, offensive capacity is increasingly displayed in attempts to intimidate other actors, influence decision-making or restrict their freedom of movement. The latter component, hostile intentions, is increasingly difficult to identify today, and this is highlighted by the different ways in which actors pursue and materialize their goals. One of these methods (which involves a wide range of types of actions) is the use of techniques specific to hybrid warfare (analyzed in the second part of this article).

Therefore, the growing range of threats to the international security and the adaptation of some of the classic ones to the new environment of confrontation have led in the last decade to important changes in the concepts and strategies of NATO and other regional actors (an example in this regard was the official establishment by NATO of the fifth battle environment – cyber[5]). Some of the most important challenges, discussed below, are: globalization; the confrontation between values, beliefs and perceptions; the exponential evolution of technology in all fields and subsequent development

---

[2] ***, World Economic Forum, *Global risks report 2023*, available at https://www.weforum.org/publications/global-risks-report-2023/digest/, accessed on 17.01. 2024.

[3] MORGENTHAU Hans, *Politica Între Naţiuni*, Polirom Publishing House, 2013, Iaşi, pp. 363-367.

[4] FRUNZETI Teodor, *Echilibrul ameninţării şi echilibrul de putere,* în cadrul *Sesiunii internaţionale de comunicări ştiinţifice cu participare internaţională,* 2011, Bucharest, UNAp Publishing House, p. 17.

[5] *Răspunsul UE la provocările în materie de securitate cibernetică,* available at*:* https://www.consilium.europa.eu/ro/policies/cybersecurity/, accessed on 18.01.2024.

of artificial intelligence (which gave the start of a world race to dominate this "land" with multiple opportunities); the cyber dimension (from the perspective of the intensification of actions in this a new field of battle); hybrid warfare (a phenomenon integrating the multiple tools used today by state and non-state actors in pursuit of interests).

Current challenges of the security environment and evolving prospects

Globalization as a phenomenon, predominantly describes a wide range of advantages and disadvantages for all security sectors, in particular as the ultimate beneficiary of these changes, the societal sector. Globalization therefore remains the main factor responsible for influencing the security environment. It generates multiple effects, leading to multiple variants, opportunities but also new risks, threats, vulnerabilities, constraints, limitations through all security sectors. Thus "through the processes that incumbent on them and, for the future, will generate multiple tensions that will influence, not always positively, the international security environment. Fragmentation and integration, localisation and internationalisation, centralisation and decentralisation are just some of the situations that can generate insecurity. Thus, "globalization is not only a direct and easy path to peace and stability, the ongoing phenomenon can also create many moments that threaten security"[6].

One of the most subtile disadvantages of this phenomenon relates to the "fragmentation of society by social media and the emergence of uncritical and isolated bubbles"[7]. People tend to identify themselves much more easily with other peers who share the same lifestyle, thus creating communities of different sizes in which comfort receiving, their interaction is limited to a reduced number of interest groups. At first sight, the effect of globalization, in this regard, is a positive one because it unites people who have the same preferences and thus facilitates their communication. But from the point of view of the security of the societal sector, the phenomenon is seen differently. Society is fragmented into homogeneous groups, susceptible to cognitive attacks since the most difficult part in organizing such an attack is already carried out by the masses of people themselves. They organized themselves according to the new trend and publicly exhibited their desires, wills, ideals, so further the manipulator will be waiting only for a favorable moment or he will initiate one.

[6] RICHICINSCHI Iurie, *op.cit.,* p. 106.

[7] CHIFU Iulian, *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21, Gândirea românească militară no.1 / 2020,* p. 18, available at https://gmr.mapn.-ro/webroot/fileslib/upload/files/arhiva%20GMR/2020%20gmr/2020/1%202020-%20gmr/chifu.pdf, accessed on 18.01.2024.

"In this complex, dynamic and conflictual world, **the main confrontation takes place between fundamentally different values, beliefs and perceptions**, between democracy and totalitarianism."[8] Although the time of the crusades has long passed and Jihad (in its form referring to a holy war of expansion) still has vague reminders of the Middle East, religion remains a strong bond between states, especially when it comes to the Muslim one. Muslim states, beyond their geographical position, their different interests or the political colour and/or the alliance to which they belong, express their solidarity and support regardless of the nature of the conflict. An illustration of this concept may be the conflict in Israel, where we can highlight Turkey's indirect support[9] for Hamas (through actions such as: the non-recognition of Hamas as a terrorist organization, the hosting of members of the movement, the promotion of the solution by creating a new state that includes the Muslim community in that area, or the harsh criticism of the way Israeli units fight and attacks on the way the Israeli government manages the dispute) and the support[10] of Iran (provision of weapons and information, the accommodation of the political leadership of Hamas in exile, the threating to Israel and the United States of America if the war continues in Palestine, the legitimacy of the 7 October attack, in which 1,400 people died, as in accordance with the international right to self-defense, resistance to aggression and Israeli occupation). In comparison, we can see a t North Atlantic Alliance member state and a state that is among the main threats of the NATO, sharing similar views on a conflict and offering different forms of support in this regard. So, the possibility of a division at the level of the Alliance, even on a religious basis, remains real. In this sense, NATO must strengthen its cohesion at the level of its members by reaffirming common values and interests and by expressing itself/acting unanimously within its foreign policy.

The impact of hi-tech rising on security is also, in essence, a consequence of globalization. In the societal sector there can be, as I mentioned earlier, numerous benefits on "social cohesion: solidarity, the

[8] IFTODE Florin, *Riscuri și amenințări la adresa securității contemporane*, available at https://core.ac.uk/download/pdf/229471504.pdf., accessed on 20.01.2024,

[9],*Bombardamente în centrul Fâșiei Gaza. Israelul anunță că și-ar putea extinde operațiunea în Nord* available at https://www.digi24.ro/stiri/externe/liderii-israelieni-dau-de-inteles-ca-gaza-va-fi-ocupata-dupa-razboi-netanyahu-israelul-va-fi-responsabil-de-securitatea-din-enclava-2570817, , accessed on 20.01. 2024,

[10],*Războiul Israel-Hamas/ Iranul amenință la ONU că SUA "nu vor fi cruțate" dacă războiul din Gaza continua*, available at https://www.agerpres.ro/politica-externa/2023/10/26/razboi-israel-hamas-iranul-ameninta-la-onu-ca-sua-nu-vor-fi-crutate-daca-razboiul-din-gaza-continua--1193619, accessed on 20.01.2024.

feeling of community, alienation, social fragmentation"[11], but at the same time, as a disadvantage, they can induce "the feeling of lack of privacy, altered identity – individual as well as collective, the need for dignity and respect"[12]. On the other hand, in the military sector, this trend focuses on "technologies that could be considered emerging (are already known and used, a slightly outdated concept but with potential for the development of new technologies) compared to the current status of the military arsenal/arms collection. However, most of these technologies are already quite advanced (e.g. drones, hypersonic missiles, portable sensors and autonomous systems) and are already changing modern warfare when used. "Relevant decisions on investment and critical capabilities for future combat technologies must be taken today"[13].

Artificial intelligence (AI) becomes the horizon towards which it tends, mainly by the great powers and those with tradition in the field of the development of new technologies, and therefore by everyone. AI represents the future in accordance with President Vladimir Putin's statement: "Whoever becomes a leader in AI will rule the world"[14], and its development has led to a race against the timetable (see the Development Plan for a new generation of AI, by which China wants to hold the monopoly over AI technologies by 2030)[15]. This new technology, however, involves certain negative effects such as: the real possibility of manipulating and amplifying feelings, actions; the elimination of certain professional categories from the labor market by replacing the human labor force; the creation of capabilities to alter the behavior of human beings (in the military sector)[16]; the monitoring and control of citizens[17], etc.). Therefore, the decision-makers, no matter how they resonate with this new concept, must collaborate in the development of AI in a constructive and timely way for the societal sector while limiting the inevitable negative consequences.

---

[11] CHIFU Iulian, *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21, Gândirea românească militară no.1 / 2020,* p. 13, available at https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2020%20gmr/2020/1%202020%20gmr/chifu.pdf, accessed on 18.01.2024.

[12] FUKUYAMA Francis, *Identity. Contemporary Identity Politics and the Struggle for Recongnition*, Profile books Ltd, London, 2018, p. 218., apud CHIFU Iulian, op.cit., p. 13.

[13] *Changing Security paradigm*, available at https://knowledge4policy.ec.-europa.eu/changing-security-paradigm_en, accessed on 19.01.2024.

[14] VINCENT James, *"Putin says the Nation that Leads in AI 'will be the Ruler of the World"* in The Verge, available at https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-theworld, accesed on 21.01.2024, apud ROSENBACH Eric, MANSTED Katherine, T*he Geopolitics of information*, 2019, USA, BelferCenter, p. 8.

[15] *Ibidem*, p.8.

[16] CHIFU Iulian, *op.cit*., p. 21.

[17] *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, 2019, available at https://nsiteam.com/ai-china-russia-and-the-global-order-technological-political-global-and-creative-perspectives/, accessed on 18.01.2024.

Cyber attacks are increasingly present and sophisticated. They may vary in magnitude depending on the type of the actor who is initiating the attack. Thus we distinguish[18]: persons and entities associated with state actors (the most important form of threat, high impact, targets of the type of critical networks and computer systems, attacks type APT – Advance Persistent Threat, strategic motivation), individuals and groups that carry out organized crime activities (risk of data compromise or temporary damage, direct or indirect financial motivation, types of attacks: malware, ransomware, info-stealer, crypto-jacking, sometimes even APT, especially in the financial-banking field) and people and groups of hackers with ideological, political or extremist-terrorist motivation (technological level and reduced capabilities, targeting systems with low level of cybersecurity, types: defacement, distributed denial of service, SQL injection). Nowadays, when we talk about hybrid warfare, it includes cyber attacks. (such in contemporary Ukrainian conflict)[19]. They have become indispensable for the achievement of various purposes such as: obtaining strategic information and information advantage; earning extra time for organizing their own actions; disorganizing the enemy's battle organization through disinformation and propaganda; influencing the opponent's perception and will; sabotage; espionage; economic, energy disruption; etc. Identification of the origin of a cyber attack (which almost entirely enjoys anonymity, at least in the initial phase) must be done through questions such as: What is the aim? Who's interested? Who has the resources, the necessary capabilities?

Along with the new threats mentioned above and developed, it must be said that most of the classic ones, from security strategies, remain of current relevance, only that they manifest adapted to the new security environments and using the new tools. These are: terrorism, the proliferation of conventional weapons and weapons of mass destruction of (WMD), organized crime, the exacerbation of the ethno-religious background, corruption, illegal trade, the resumption of frozen conflicts and the development of conditions for new ones, non-compliance with human rights and international humanitarian law, manipulation of refugee flows/migration, aggressive offensive behavior of international actors, strengthening of military potential in the vicinity of NATO, hostile information actions, distortions of energy markets, etc.

At the same time, the new threat range is characterized by a number of concepts used, such as: emerging, disruptive, unconventional, asymmetric, information, cognitive and hybrid attacks, which must be well delimited from

[18]*Strategia de securitate cibernetică a României (2022-2027)*, 2022, Bucharest, Monitorul Oficial al României, pp. 8-9.

[19] HASRATYAN Nina, *Cyberattacks in hybrid warfare: the case of Russia/Ukraine War*, 2022, available at https://www.headmind.com/en/cyberattacks-hybrid-warfare/, accessed on 18.01.2024.

a theoretical point of view before any security analysis. The concept with which it is operated most often today, and which encompasses most of the others, is that of hybrid warfare, a modern and effective warfare through the prism of the exploitation of multiple instruments of power both vertically and horizontally, the hybrid threats being at the base "an umbrella term encompassing a wide variety of existing adverse circumstances and actions"[20].

Hybrid warfare – the main form of current threats manifestation

The origins of the term hybrid war, in theory, rise in the US (Gl. Lt. James Mattis and Frank Hoffman, 2005), NATO showing its interest in this much later, but, in practice, the real rise of this new concept occurs with the outbreak of the conflict between the Russian Federation and Ukraine. So the reference point for the study of the hybrid war remains the annexation of Crimea by Russia (2014). Thus "public opinion and political classes in NATO countries have begun to pay attention to hybrid threats. An astonished international community watched unmarked military units and local actors take over the peninsula. By exploiting the socio-political divisions of the region and launching a multi-channel disinformation campaign inside and outside Ukraine, Moscow managed to hide its objectives and plausibly deny responsibility until the invasion was completed. The Russian invasion of Donbas (2014) confirmed this fading of the borders between peace and war in a large grey area that was a natural habitat for disinformation and cyber attacks. Since then, these asymmetric, ambiguous instruments, which are difficult to attribute and can have an impact on society as a whole, have been observed by both NATO and the European Union"[21].

The grey zone, this vacuum between the two dimensions, peace and war, is increasingly being exploited. Hybrid warfare can escalate horizontally, vertically or combined, depending on the instruments used by the actors.

[20] FRIDMAN Ofer, KABERNIK Vitaly and PEARCE James, *Hybrid conflicts and information warfare – new labels, old politics*, 2019, USA, Lynne Rienner Publishers, p. 71.
[21] PIELLA Colom Guillem, *NATO's strategies for responding to hybrid conflicts,* 2022, , available at https://www.cidob.org/en/articulos/cidob_report/n_8/nato_s_strategies_for_-responding_to_hybrid_conflicts, accessed on 20.01.2024.

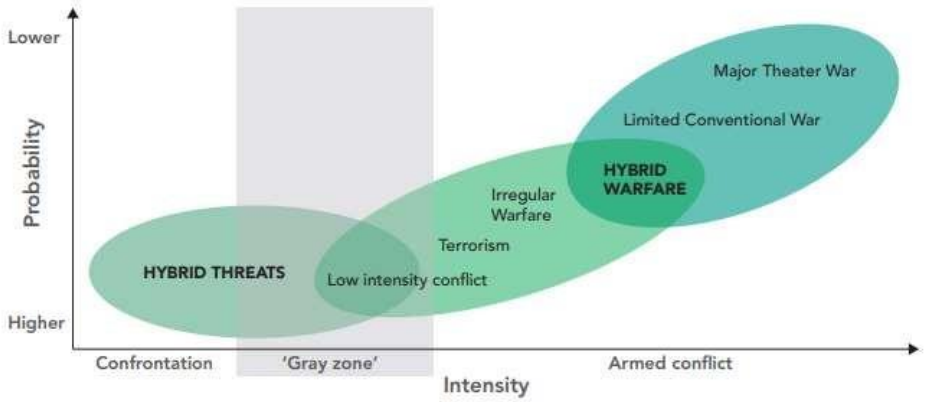

Figure 1: *Hybrid Threats and Hybrid Warfare Shown on a Continuum of Conflict*[22]

The actuality of hybrid warfare and the possibility of manifesting threats since peacetime, without a clear demarcation on the source, means and end goal pursued, have led to "an increase in strategic revisionism and the proliferation of grey zones in which the hybrid will continue to play a fundamental role"[23]. However, international actors are beginning to understand this phenomenon more and more, to attach due importance to it and to identify new ways of managing it.

Therefore, NATO members face state and non-state actors that generate threats and challenges by using "hybrid activities to target political institutions, to influence public opinion and to undermine the security of NATO citizens. Hybrid methods of warfare – such as propaganda, deception, sabotage, and other non-military tactics – have long been used to destabilize opponents. What is new about the attacks observed in recent years is their speed, scale and intensity, facilitated by rapid technological changes and global interconnectivity"[24]. Thus, as is apparent from the previous statement, hybrid actions would not be successful if in advance "the susceptibility of States to such attacks, which is given primarily by vulnerabilities, had not been speculated"[25]. In the broad understanding of some specialists, this model of application of hybrid actions is rather used by totalitarian states which

[22] MONAGHAN Sean, *Countering Hybrid Warfare So What for the Future Joint Force*, 2018, available at https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf, accessed on 21.01.2024.
[23] PIELLA Colom Guillem, *op.cit.*, 2022, available at https://www.cidob.org/en/articulos/-cidob_report/n_8/nato_s_strategies_for_responding_to_hybrid_conflicts, accessed on 20.01.2024.
[24] *Countering Hybrid Threats*, available at https://www.nato.int/cps/en/natohq/-topics_156338.htm, accessed on 20.01.2024.
[25] *Countering Hybrid Threats*, available at https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en, accessed on 21.01.2024.

consider the multitude of rights and freedoms conferred by democracy as weaknesses of the state and are exploited as future targets.

One of the models by which possible targets can be identified in the case of hybrid attacks is "MICEPIO (Military, Information, Cultural, Economic, Political, Infrastructure, Other forms), which supports identifying the use of cultural instruments, such as religion or sports, as a tool for hybrid influencing, successful target selection and operationalization of the selection demands an in-depth understanding of the target society and availability of necessary means and tools"[26]. Therefore, the most effective understanding of the target society in order to identify those groups susceptible to such an attack is achieved from time of peace with the help of intelligence structures that provide from within the territory of the opponent key information. Its usually are: where the use of these mechanisms is reasonable, the timing for producing the expected effects, the structure of the message accepted, the sources that can be corrupt for the distribution of information and the computer means most frequently used by the local population. In other words, a thorough analysis is needed to answer the questions: Who? What? Where? How? When? Why? in order for a cognitive attack to produce maximum effect.

Hybrid threats enjoy great success as their effectiveness is guaranteed by a number of features, such as[27]:

- coordination and synchronization;
- deliberately target democratic states and institutions; and economic vulnerabilities;
- use a wide range of means;
- exploit the thresholds of detection and attribution as well as the border between war and peace;
- aim to influence different forms of decision-making at the local (regional) state or institutional level.

Following the conflict in Ukraine, which is still underway, the main types of threats associated with the hybrid war can be extracted: disinformation, propaganda, psychological/cognitive attacks (influencing the perception/will of the public), economic pressure (mainly relieved by energy dependence), exacerbating the sense of insecurity in the social environment, diffuse military actions (in sight or masked by concealing the identity of the military) carried out at the boundary of the law (legislative gaps) and borders, electoral interventions, guiding migratory flows, cyber attacks, etc. These actions combined with classical armed fighting generate hybrid threats that

[26] *What are hybrids threats,* available at https://www.linkedin.com/pulse/what-hybrid-threats-pasi-eronen, accessed on 19.01.2024.

[27] TERRADOS Jose Juan, *Hybrid Warfare*, in *The Three Swords Magazine 35/2019,* p. 45, available at https://www.jwc.nato.int/images/stories/threeswords/HybridWar_Dec2019.pdf, accessed on 20.01.2024.

"propagate multi-vectorially, show a high degree of synchronization and generate nonlinear effects that are difficult to evaluate quickly"[28]. The materialization of these actions, and not only, is possible as a result of a sum of factors that contributed to their emergence:[29]

- change of the post-Cold War international order. In the new international system, "the power to change beliefs, attitudes, preferences, opinions, expectations, emotions and/or predispositions to act is more important today than material power". Today, the world is experiencing the "dark side of globalization", the role of the nation-state is being questioned, as are alliances with norms and rules that limit responses to asymmetric-type antagonistic actions.
- globalization, advanced communications technologies and explosive developments in the online environment are contributing significantly to increasing the operational potential of state actors, but also of non-state actors (such as, for example, multinational corporations, hacking groups, terrorist groups, etc.) in less established operational areas, such as cyber and information.
- the emergence of new areas of confrontation, such as the cyber, where the "rules of the game" have not yet been created. With the exception of cyber tools and technologies, most of the tools used in hybrid conflicts – such as propaganda and political-diplomatic or economic actions, for example – are not new. The actions carried out in cyberspace offer both new tools of action (with, for example, cyber espionage, poisoning with fake news), but also new opportunities for maximizing the effect of traditional instruments of influence (politico-diplomatic, economic, information, etc.).
- exploiting the potential of new media technologies as well as new tools of social influence. The high speed of information flow, the way information is produced and how social communities can connect across national borders are the result of digitization and the development of social media tools. Confidence, one of the fundamental pillars of advanced democratic societies, is eroding under the influence of modern techniques of manipulation. The Internet has become the new

[28] FRUNZETI Teodor, Bărbulescu Cristian, *Rezilienţa naţională la ameninţările hibride şi cultura de securitate. Un cadru de analiză,* available at https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, accessed on 21.01.2024.
[29] *Ibidem* p. 4.

"field of confrontation", and propaganda, disinformation and fake news are the new weapons of warfare.

- clear delimitation between peace and war is becoming increasingly difficult to notice. The prevalence for the use of unconventional means makes the target of the new type of aggression not aware of the state of war in which it is, until the use, concealed or on a small scale, of the military instrument (the case of Ukraine).

Countering hybrid threats within international organizations remains a constant concern. Currently, the EU strategy[30] in this regard is based on four pillars: early warning, resilience, response (from the use of the diplomatic instrument to the application of force), cooperation, and, NATO strategy[31] incorporates three fundamental elements: preparedness, deterrence, defense. Alongside these theoretical tools, institutions specialized in combating hybrid threats have been created such as: European Centre of Excellence for Countering Hybrid Threats (EU); Innovation, hybrid and cyber division (NATO); Cooperative Cyber Defense; etc. and the military train within scenarios adapted to new trends such as the annual exercise Cyber Coalition. Thus, cooperation at NATO and EU level, in order to counteract these types of threats, must continue to be based on dialogue and cooperation, be complementary, be conducted both at the political and operational level, while realizing that future conflicts will take place both between people and, above all, among people.

Conclusions

The current international security environment captures a trend that describes a diverse range of methods used by different actors to identify and exploit the vulnerabilities of individuals, populations, states, national and international organizations. Today, more than ever, emphasis is placed on the analysis stage of the opponent: identifying security breaches, tracking how it adapts or not to certain phenomena taking place on a large scale, how society acts to cognitive attacks, developing scenarios and only then acting accordingly. The intelligence structures have gained more and more weight, and the strategic information exploited in time, can be more important than the actual military action that follows, as it creates the information advantage, strategic surprise and the opponent will become one unprepared or paralyzed. The effects will therefore be greater with fewer costs.

Thus, the main challenges to the security environment, pursued with interest by the actors, remain those related to certain phenomena whose

[30] Strategia UE de combatere a războiului hibrid, available at https://ec.europa.eu/-commission/presscorner/detail/it/MEMO_16_1250, accessed on 22.01.2024.

[31] Strategia NATO de combatere a războiului hibrid, available at https://www.nato.int/-cps/en/natohq/topics_156338.htm, accesssed on 22.01.2024.

development is inevitable, for example: globalization; the confrontation between values, beliefs and perceptions; the fulminant evolution of technology in all fields and subsequently the development of artificial intelligence; the cyber dimension and hybrid warfare. In a certain context, multiple components of these challenges can work together to materialize a hybrid action (which remains one of the biggest threats). A hypothetical example of this, would be a cyber attack that illegally spreads, across several social networks, misinformation messages about a possible government AI development program in the economic sector, which will drastically reduce the human labor force. The result is easily understood, destabilizing the social, economic and political sectors, with the aim of discrediting the form of government. At the same time, it must be understood that often cyber-attacks of this type (cognitive) can be carried out in cascade, layer after layer, with the aim of changing perception and will in the long term. They can be part of a broader strategy that eventually culminates in a large-scale attack, generating, for example, a revolt, a coup d'état.

Based on what was argued in the article, recently crystallized in specialized studies, a new concept, the social resilience, is noted, which becomes a basic solution in order to limit the effects of new threats, especially those describing cognitive attacks. Society, related institutions and policymakers must be educated on a culture of security, be aware of new risks and threats, and thus, developing resilience helps to limit and even eliminate vulnerabilities. One of the main advantages of real resilience is by definition, the system's ability to take shocks, reject some of them, and sometimes return to its original state. This capacity is directly proportional to generating additional time for the organization and implementation of an appropriate response to the threat in question. Further analysis of this new concept can become a further direction of research, answering the following research questions: *What is the applicability of resilience development? Can social resilience be developed integrated at the regional level or only at the state level due to the presence of distinct peculiarities such as politics, identity, system of values and beliefs, etc.? What are the foundations of social resilience. Can they be influenced in order to design it incorrectly?*

BIBLIOGRAPHY

CHIFU Iulian, *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21, Gândirea românească militară no. 1*

2020, available at: https://gmr.mapn.ro/webroot/fileslib/upload/-files/arhiva%20GMR/2020%20gmr/2020/1%202020%20gmr/chifu.pdf

IFTODE Florin, *Riscuri și amenințări la adresa securității contemporane,* available at: https://core.ac.uk/download/pdf/229471504.pdf

FRIDMAN Ofer, KABERNIK Vitaly and PEARCE James, *Hybrid conflicts and information warfare – new labels, old politics*, 2019, USA, Lynne Rienner Publishers.

FRUNZETI Teodor, *Echilibrul amenințării și echilibrul de putere,* în cadrul *Sesiunii internaționale de comunicări științifice cu participare internațională,* 2011, București, UNAp Publishing House;

FRUNZETI Teodor, Bărbulescu Cristian, *Reziliența națională la amenințările hibride și cultura de securitate. Un cadru de analiză, Impact Strategic,* 2018, available at: https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf

FUKUYAMA Francis, *Identity. Contemporary Identity Politics and the Struggle for Recongnition*, Profile books Ltd, London, 2018.

HASRATYAN Nina, *Cyberattacks in hybrid warfare: the case of Russia/Ukraine War*, 2022, available at: https://www.headmind.-com/en/cyberattacks-hybrid-warfare/

MONAGHAN Sean, *Countering Hybrid Warfare So What for the Future Joint Force,* 2018, available at: https://ndupress.ndu.edu/-Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf

MORGENTHAU Hans, *Politica Între Naţiuni*, Polirom Publishing House, 2013, Iaşi.

PIELLA Colom Guillem, *NATO's strategies for responding to hybrid conflicts,* 2022, available at: https://www.cidob.org/en/articulos/-cidob_report/n_8/nato_s_strategies_for_responding_to_hybrid_conflicts

RICHICINSCHI Iurie, Riscuri și amenințări potențiale la adresa securității internaționale, 2016, available at: https://ibn.idsi.md/sites/-default/files/imag_file/105_112_Riscuri%20si%20amenintari%20potentiale%20la%20adresa%20securitatii%20internationale.pdf

TERRADOS Jose Juan, *Hybrid Warfare,* in *The Three Swords Magazine 35/2019,* available at: https://www.jwc.nato.int/images/-stories/threeswords/HybridWar_Dec2019.pdf

VINCENT James, *"Putin says the Nation that Leads in AI 'will be the Ruler of the World"* in The Verge, available at: https://www.theverge.com-/2017/9/4/16251226/russia-ai-putin-rule-theworld apud ROSENBACH Eric, MANSTED Katherine, T*he Geopolitics of information*, 2019, USA, Belfer Center.

Strategia UE de combatere a războiului hibrid, available at: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 Strategia NATO de combatere a războiului hibrid, available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

Strategia de securitate cibernetică a României (2022-2027), 2022, București, Monitorul Oficial al României.

Răspunsul UE la provocările în materie de securitate cibernetică, available at: https://www.consilium.europa.eu/ro/policies/cybersecurity/

Countering Hybrid Threats, available at: https://www.eeas.europa.eu/-eeas/countering-hybrid-threats_en;

What are hybrids threats, available at: https://www.linkedin.com/pulse/what-hybrid-threats-pasi-eronen;

World Economic Forum, *Global risks report 2023*, available at: https://www.weforum.org/publications/global-risks-report-2023/digest/

Changing Security paradigm, available at: https://knowledge4policy.-ec.europa.eu/changing-security-paradigm_en;

Bombardamente în centrul Fâșiei Gaza. Israelul anunță că și-ar putea extinde operațiunea în Nord, available at: https://www.digi24.ro/-stiri/externe/liderii-israelieni-dau-de-inteles-ca-gaza-va-fi-ocupata-dupa-razboi-netanyahu-israelul-va-fi-responsabil-de-securitatea- din-enclava-2570817

Războiul Israel-Hamas/ Iranul amenință la ONU că SUA "nu vor fi cruțate" dacă războiul din Gaza continua, available at: https://www.agerpres.ro/politica-externa/2023/10/26/razboi-israel-hamas-iranul-ameninta-la-onu-ca-sua-nu-vor-fi-crutate-daca-razboiul-din-gaza-continua--1193619

AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, 2019, available at: https://nsiteam.com/ai-china-russia-and-the-global-order-technological-political-global-and-creative-perspectives/ .