HYBRID WAR – A REALITY OF THE CONTEMPORARY WORLD; CONCEPT, MODEL, IMPLICATIONS

Ph.D. Student, Corneliu-George IACOB
University of Economic Studies, Bucharest, Romania
E-mail: iacobcorneliu2022@gmail.com

Abstract: *The current global security environment is characterized by high complexity, with hybrid threats and hybrid warfare being its defining features. Understanding the true dimension of modern warfare means outlining the typology of hybrid threats, clarifying the concept of hybrid warfare and, last but not least, highlighting the role of various state and non-state actors in the dynamics of global power relations. In recent decades, the North Atlantic Treaty Organization (NATO) has delivered innovative strategic concepts in efforts to combat hybrid threats. The purpose of this article is to establish a conceptual basis for describing hybrid threats and to analyze the role of NATO and the US in shaping the global security environment, pointing out the evolution of NATO's strategic concept of security and presenting US strategic options for the future of the security environment in the perspective of 2035.*

Keywords: *hybrid threats, hybrid warfare, global security environment, NATO, strategic concept*
JEL Classification: *F51, F53.*

1. Introduction

In Today, at mid-century, great powers and rising challengers alike have converted hybrid combinations of economic power, technological prowess and virulent, cyber-enabled ideologies into effective strategic strength. They apply this strength to disrupt or defend the economic, financial, social, and cultural foundations of the old liberal order. They assert or dispute regional alternatives to established global norms. State and non-state actors compete for power and control, often below the level of traditional armed conflict – or shield and protect their activities with escalatory nuclear options and doctrines. Strife, conflict, and war remain endemic in mid-century and the ways in which wars are fought have undergone a significant evolution – nowhere more so than in the land domain. (TRADOC,2015)

"Future conflicts will increasingly emphasize the disruption of critical infrastructure, societal cohesion, and basic government functions in order to secure psychological and geopolitical advantages, rather than the defeat of enemy forces on the battlefield through traditional military means." (National Intelligence Council, 2017)

If war as a human activity is hybrid by nature, the combination of regular and irregular modes of fighting in a single maneuver can prove a formidable weapon against a "single-mode" opponent. In its regular component, hybrid maneuver requires the opponent to concentrate forces in order to maximize firepower — a basic principle of regular warfare. At the same time, the maneuver's irregular component compels him to disperse these same forces, so they can protect the rear and supply lines. Of course, this dilemma of concentration vs. dispersion can only play to the advantage of the hybrid fighter if he is able to leverage greater operational mobility, either by splitting his forces in two well-coordinated components or by acting in a swarm-like fashion, i.e. to converge rapidly on a target, attack and then re-disperse. Military history offers three main types of operations where such patterns provided added value at the operational level of war: compound warfare, techno-guerrilla warfare and protracted warfare.(Tenenbaum 2015,102)

In 2005, British General Rupert Smith wrote: "War no longer exists. Confrontation, conflict and struggle undoubtedly exist all over the world ... and the state still has armed forces that it uses as a symbol of power. The phrase "new war" brings a number of asymmetries:

- in objectives (which are less clear because they are less connected to the paradigm of interstate warfare);
- in time (because these wars tend to be timeless);
- between the protagonists (because they tend to involve a variety of state actors as well as non-state actors);
- in combat modes (a mixture of traditional and new weapons and tactics is used; it erodes the distinction between combatants and non-combatants).
- in space (there is no longer a distinction between "front" and "back" or "war on the front" and "front at home", the battle is everywhere, often simultaneously).

This type of war can be called "asymmetric warfare", "compound warfare" or "irregular wars", "small or guerrilla warfare", depending on the definitions of different authors from different eras and the distinct characteristics highlighted. (Marcuzzi, 2018).

The literature analyzes the concept of hybrid threats as well as that of hybrid warfare. Reference works for this study area are (Tenenbaum, 2015), (Marcuzzi, 2018), (European Commission, 2021), (European Commission, 2016), (Cullen, P. et al., 2021), (Gressel, 2019), (Weissmann, 2019), (Balaban & Mielniczek, 2018), (Cullen,P. Et al. 2016), (Rühle & Roberts, 2021), (Kamp, 2016), these also presenting various analysis models. The present study presents, as a novelty, essential conceptual delimitations regarding the notion of hybrid war, also highlighting the position of NATO and the USA in relation to these developments in the international economic environment.

In the current international environment, hybrid war and hybrid threats occupy a special place and are part of the broad area of global analyzes of developments in the world economy and trends in the redefinition of power centers. The main research objective of this study is to highlight a model of analysis regarding the hybrid war and, at the same time, to emphasize the attitude adopted by NATO and the US towards the events taking place in the world economy in order to increase the level of economic security, reducing the risks geopolitical and geoeconomic.

The research methodology uses various methods: the logical analysis method, the systemic method, the comparative method, the historical method and the situation analysis. The study period covers the time interval from the Second World War to the present. Historical analysis and situational analysis used in geopolitical theory are used to observe and research the geopolitical area to highlight the nature and intensity of interests that actors have at a given time in a geographic space and their place in a power equation.

2. Hybrid threats: concept and typology

The European Centre of Excellence for Countering Hybrid Threats outlines hybrid threats with the next focus: ″The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.

Hybrid action is characterized by ambiguity as hybrid actors blur the usual borders of international politics and operate in the interfaces between external and internal, legal and illegal, and peace and war. The ambiguity is created by combining conventional and unconventional means – disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare. ″ (European Commission, 2021)

Hybrid CoE characterizes hybrid threats as:

- Coordinated and synchronized action that deliberately targets democratic states' and institutions'systemic vulnerabilities through a wide range of means.
- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).
- Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target. (European Commission, 2021)

Hybrid threats can be characterized as a mixture of coercive and subversive activity, conventional and unconventional methods (eg diplomatic, military, economic, technological, informational), which can be used in a coordinated manner by the state or state actors to achieve objectives. remaining at the same time below the threshold of open organized hostilities. Emphasis is usually placed on exploiting the vulnerabilities of the target and on generating ambiguity with the intention of impeding decision-making processes. Massive disinformation campaigns, using social networks to control the political narrative or to radicalize, recruit and direct different actors can be vehicles for hybrid threats. (European Commission, 2016).

„The conceptualization of the hybrid threat-hybrid war relationship is based on the conceptualization of the war/hybrid war from the previous academic literature. The terms hybrid threats and hybrid warfare are sometimes used interchangeably, which is one of the reasons why concepts may seem confusing. In addition, the concepts were examined through various disciplinary objectives: international relations, strategic studies, security studies, military studies, history and political science. This multidisciplinary analytical mosaic also blurs the image of what the concept of hybrid threats actually entails. In a certain approach, the concept of hybrid threats is used as an umbrella concept, while hybrid warfare / war is part of the activity that takes place under the umbrella of hybrid threats (cause-effect ratio). According to Frank Hoffman, who focused on non-state actors such as Hezbollah and al-Qaeda, their tactical and operational military activities are directed and coordinated in the main battlefield to achieve synergistic effects and to include tactics used by transnational networks. When Frank Hoffman began using the label "hybrid warfare", it was just one of many labels, which included "new warfare", fourth-generation warfare, and asymmetric warfare; they were used by analysts to conceptualize the changes in contemporary warfare, in line with the idea that warfare has become "substantially distinct" from older patterns of conflict. There are a lot of other concepts that describe new forms of conflict/war: "surrogate war", "gray area activity", "raid", "unrestricted war" (Chinese origins), "reflexive control" (Russian origins), "New generation war" (Russian origin), "conflict-free competition", "active measures" (Russian origin), "non-linear war", "asymmetric war", "composite war", "ambiguous war", "political war", "Information warfare", "cyber warfare" - all trying to describe actions very similar to the concept of hybrid threats - interventions and operations against states and institutions. "(Cullen, P. et al.,2021).

The term "hybrid threat" is presented in different ways, both in official documents of countries / international organizations and in the literature. For example, NATO considers that hybrid threats combine military and non-military means, as well as hidden and obvious means, including misinformation, cyber attacks, economic pressure, the deployment of irregular armed groups and the use of regular forces; NATO sees hybrid threats as those posed by adversaries, with the ability to simultaneously use conventional and unconventional means in an adaptive way to achieve its goals. "(Gressel, 2019).

There are four main pillars that need to be examined in order to build a full understanding of the concept of hybrid threats:

- Stakeholders (and their strategic objectives);
- Tools used;
- Areas targeted;
- Phases (including the types of activity observed in each phase);

The analytical framework of the conceptual model, which captures the pillars mentioned above and demonstrates their connections in a dynamic way, can be used in different perspectives. An actor (state or non-state), who has objectives but limited abilities or limited possibilities to achieve them, can apply a variety of tools to a series of domains to perform a certain type of activity, to achieve a series of tasks. objectives and affects the target. This model, combined with quantitative information from information, media monitoring tools, as well as other sources of information, can be transformed into a comprehensive risk assessment and resilience tool, which can provide a holistic picture of the security position. of a country against hybrid threats. A more detailed typology of hybrid threats can be found in Table 1. The typology of hybrid threats, reiterating that "the hybrid is always a combination of tools, but not all combinations are hybrid" (Cullen, P. et al.,2021).

Table no. 1 Typology of hybrid threats

Tools	Affected domains
Physical operations against infrastructure	Infrastructure, Economy, Cyber, Space, Military/Defence, Information, Social/Societal, Public Administration
Creating and exploiting infrastructure dependency (including civil-military dependency)	Infrastructure, Economy, Cyber, Space, Military/Defence, Public Administration
Creating or exploiting economic dependencies	Economy, Diplomacy, Political, Public Administration
Foreign direct investment	Economy, Infrastructure, Cyber, Space, Military/Defence, Public Administration, Intelligence, Information, Political, Legal
Industrial espionage	Economy, Infrastructure, Cyber, Space, Intelligence, Information
Undermining the opponent's national economy	Economy, Public Administration, Political, Diplomacy
Leveraging economic difficulties	Economy, Public Administration, Political, Diplomacy
Cyber espionage	Infrastructure, Space, Cyber, Military/Defence, Public Administration
Cyber operations	Infrastructure, Space, Cyber, Social/Societal, Public Administration, Military/Defence
Airspace violation	Military/Defence, Social/Societal, Political, Diplomacy
Territorial water violation	Military/Defence, Social/Societal, Political, Diplomacy

Weapons proliferation	Military/Defence
Armed forces conventional/sub-conventional operations	Military/Defence
Paramilitary organizations (proxies)	Military/Defence
Military exercises	Military/Defence, Diplomacy, Political, Societal
Engaging diasporas for influencing	Political, Diplomacy, Social/Societal, Culture, Intelligence, Information
Financing cultural groups and think tanks	Societal, Culture, Political, Diplomacy
Exploitation of sociocultural cleavages (ethnic, religion and culture)	Social/Societal, Culture
Promoting social unrest	Infrastructure, Social/Societal, Economy, Political
Manipulating discourses on migration to polarize societies and undermine liberal democracies	Social/societal, Culture, Political, Legal
Exploiting vulnerabilities in public administration (includingemergency management)	Public Administration, Political, Social/Societal
Promoting and exploiting corruption	Public Administration, Economy, Legal, Social/Societal
Exploiting thresholds, non-attribution, gaps and uncertainty in the law	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Leveraging legal rules, processes, institutions and arguments	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Intelligence preparation	Intelligence, Military/Defence
Clandestine operations	Intelligence, Military/Defence
Infiltration	Intelligence, Military/Defence
Diplomatic sanctions	Diplomacy, Political, Economy
Boycotts	Diplomacy, Political, Economy
Embassies	Diplomacy, Political, Intelligence, Social/Societal
Creating confusion or a contradictory narrative	Social/Societal, Information, Diplomacy
Migration as a bargaining chip in international relations	Social/Societal, Diplomacy, Political
Discrediting leadership and/or candidates	Political, Public Administration, Social/Societal
Support of political actors	Political, Public Administration, Social/Societal
Coercion of politicians and/or government	Political, Public Administration, Legal
Exploiting immigration for political	Political, Social/Societal

influencing	
Media control and interference	Information, (Media) Infrastructure, Social/Societal, Culture
Disinformation campaigns and propaganda	Social/Societal, Information, Political, Cyber, Culture, Public Administration
Influencing curricula and academia	Social/Societal, Culture
Electronic operations (GNSS jamming and spoofing)	Space, Cyber, Infrastructure, Economy, Military/Defence

Source: Cullen, P. et al.,2021, p.7

3. Hybrid warfare: concept and model of analysis

Hybrid warfare is not new; the means of waging it have evolved and simply expanded into all dimensions of state and society. Schmid Johann in Der Archetypus hybrider Hybride Kriegfuhrung vs.militarisch zentrierte Kriegfuhrung see: There is no universally-accepted definition of hybrid warfare that leads to some debate whether the term is useful at all. Some argue that the term is too abstract and only the latest term to refer to irregular methods to counter a conventionally superior force. The abstractness of the term means that it is often used as a catch all term for all non-linear threats. Hybrid warfare is warfare with the following aspects:

✓ A non-standard, complex, and fluid adversary. A hybrid adversary can be state or non-state. The main adversaries are non-state entities within the state system. The non-state actors can act as proxies for countries but have independent agendas as well.

✓ A hybrid adversary uses a combination of conventional and irregular methods. Methods and tactics include conventional capabilities, irregular tactics, irregular formations, diplomacy, politics, terrorist acts, indiscriminate violence, and criminal activity. A hybrid adversary also uses clandestine actions to avoid attribution or retribution. The methods are used simultaneously across the spectrum of conflict with a unified strategy.

✓ A hybrid adversary is flexible and adapts quickly. For example, the Islamic State's response to the US aerial bombing campaign was a quick reduction of the use of checkpoints, large convoys, and cellphones. Militants also dispersed among the civilian population. Civilian collateral damage from airstrikes can be used as an effective recruiting tool.

✓ A hybrid adversary uses advanced weapons systems and other disruptive technologies. Such weapons can be now bought at bargain prices. Moreover, other novel technologies are being adapted to the battlefield such as cellular networks.

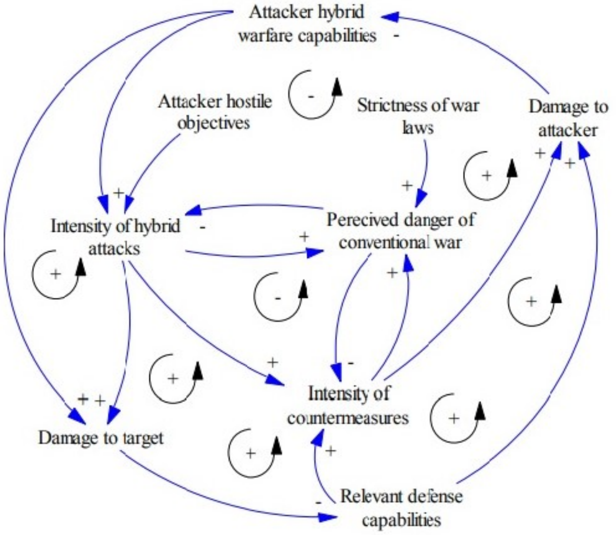
✓ Use of mass communication for propaganda. The growth of mass communication networks offers powerful propaganda and recruiting tools. The use of fake news websites to spread false stories is an element of hybrid warfare.

✓ A hybrid war takes place on three distinct battlefields. They are the conventional battlefield, the indigenous population of the conflict zone, and the international community.(Schmid, 2020)

Hybrid warfare is a concept very close to irregular warfare and asymmetric warfare. Hybrid warfare and asymmetric warfare can be seen as two sides of the same coin. They may look different, but in reality they are very similar. Asymmetric warfare refers to compensating for one's own military and organizational weakness compared to one's adversary. This feature is shared by hybrid warfare, although it is a generally broader concept and less related to one's own organization. Irregular warfare is also similar, with the main difference between asymmetric warfare and hybrid warfare being related to who is waging the war. Unlike the other two concepts, it is built on the presence of a non-state actor - normally a form of insurgent or terrorist actor; with some, the goal is to gain political power to bring about political, social, economic and / or religious change; this concept is often used in a broad and careless manner, referring to a wide range of indefinite warfare that is not a conventional warfare. In conclusion, hybrid warfare refers to an asymmetric warfare under a new label. Hybrid warfare itself is just one of a variety of terms used to describe this phenomenon, in which "sixth generation war", "contactless war", "new war", "next generation war", "ambiguous war" "," Asymmetric warfare "," nonlinear warfare "and" full spectrum conflict "are examples of more or less synonymous terms. Although there is not much new in the concept itself, it is a useful tool to think about the wars of the past, the wars of today and the wars of the future. (Weissmann, 2019).

A possible representation of hybrid conflicts is proposed by :(Balaban & Mielniczek, 2019)

Figure no. 1. Concept of hybrid conflicts


Attacker hybrid warfare capabilities
Attacker hostile objectives
Strictness of war laws
Damage to attacker
Intensity of hybrid attacks
Perecived danger of conventional war
Intensity of countermeasures
Damage to target
Relevant defense capabilities

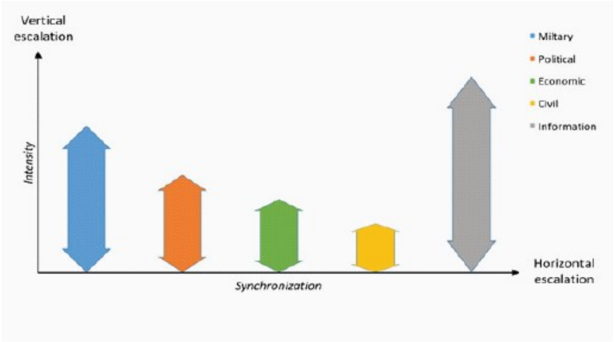
Source: adapted from Balaban & Mielniczek, 2018, p. 373-374

The perceived danger of conventional warfare increases with the increasing intensity of hybrid attacks and the increasing intensity of countermeasures, but it also generates feedback links that reduce both causal factors. Deterioration of the target has a negative effect on its relevant defense capabilities, which has a positive relationship with the intensity of countermeasures. Both the intensity of countermeasures and the relevant defense capabilities have a positive relationship with the attacker's damage. Finally, the greater the attacker's damage, the lower the attacker's hybrid warfare capabilities, which have a positive relationship to the target's damage. With only nine factors at a very high level, this conceptual model has eight dynamic loops: six reinforcements and two balances. Not surprisingly, this indicates a high dynamic complexity of the system. (Balaban & Mielniczek, 2018)

The Russian military has developed a strategy it calls the "New Generation War," which combines "asymmetrical, nonlinear, unconventional tactics with modern forms of traditional warfare." Although each of the individual tactics is not new in itself, "their combination - stimulated by modern technology - makes it different."

A model of hybrid warfare is made by: (Cullen, P., 2016). The model depicts how a HW actor uses its instruments of power (MPECI: military, political, economic, civilian and informational) across the PMESII (political, military, economic, societal, informational and infrastructure) vulnerabilities of a target system, to escalate – vertically and horizontally – to achieve the desired goals.

Figure no. 2. The hybrid warfare model



Source: adapted from Cullen, P. et.al., 2016, p.2-4

"Hybrid" refers not only to the means (or combination of means), but also to how these are employed in a highly coordinated and synchronized fashion to create synergistic effects beyond the immediate element of power. This synchronization has the effect of acting as a force multiplier. This, in turn, assumes that HW requires or at least can leverage a high degree of centralized operational command and control and strategic coordination of the elements of power, and not only a unity of effort among the elements. As the figure shows, the means (the elements of power) may be vertically escalated or de-escalated (increased/decreased intensity), or horizontally escalated or de-escalated (synchronization of elements of power creating effects that can have the same impact as vertical escalation of one mean, without necessarily overstepping the opponent's response thresholds) – or a combination of the two, to achieve a goal. (Reichborn-Kjennerud & Cullen, 2016)

Hybrid warfare reflects a wide range of activities that state and non-state actors undertake to gain political, military, economic, social, intelligence, infrastructure, physical environment and time benefits (PMESII-PT). Not surprisingly, both now and throughout history, political and military leaders have sought the best ways to achieve their goals and considered the advantages and disadvantages of each action, including those perceived as disgraceful.

4. The role of NATO and the USA in shaping the global security environment

Addressing hybrid threats is a long-term strategic challenge for NATO and allies. To meet this challenge, the rigorous planning and decision-making processes that have characterized post-Cold War crisis response operations need to be moved away from a more dynamic approach, in which debate, political reflection, decision-making and control are based. on a constantly updated picture of the situation. For reasons of efficiency, NATO considers each actor using hybrid practices as a separate entity, driven by its own strategic motivations. By taking a more targeted approach, NATO is better able to discourage potential aggressors from engaging in hybrid campaigns, making them understand that they have more to lose than to gain, and is also better equipped to act on the new ground. confrontation that constitutes the "Gray Zone" (Rühle & Roberts, 2021)

International cooperation and solidarity are important tools for strengthening, discouraging, understanding the threat and building resistance. It is no coincidence that the EU and NATO have developed new sets of tools to address hybrid threats.

One of the core reasons that have made NATO the most successful security alliance in recent history is its ability to adapt to a changed political environment, updating the Atlantic Alliance's strategic foundations in doing so. In the Alliance's 70-year history only seven such documents, traditionally entitled "Strategic Concepts," have been issued: in 1950, 1952, 1957, 1967, 1991, 1999 and, most recently, in 2010.(Kamp, 2016)

The Strategic Concept is an official document that outlines NATO's enduring purpose and nature, and its fundamental security tasks. It also identifies the central features of the new security environment, specifies the elements of the Alliance's approach to security and provides guidelines for the adaptation of its military forces. Strategic Concepts equip the Alliance for security challenges and guide its future political and military development. They reiterate NATO's enduring purpose and nature, and its fundamental security tasks and are reviewed to take account of changes to the global security environment to ensure the Alliance is properly prepared to execute its core tasks, making transformation in the broad sense of the term, a permanent feature of the Organization.

The current Strategic Concept "Active Engagement, Modern Defence" (2010) outlines three essential core tasks – collective defence, crisis management and cooperative security.

At the Brussels Summit, in June 2021, NATO Leaders agreed to develop the next Strategic Concept in time for the next summit in 2022. Over time, the Alliance and the wider world have developed in ways that NATO's founders could not have envisaged, and these changes have been reflected in each and every strategic document that NATO has ever produced.

The 2010 Strategic Concept "Active Engagement, Modern Defence" is a very clear and resolute statement on NATO's core tasks and principles, its values, the evolving security environment and the Alliance's strategic objectives. After having described NATO as "*a unique community of values committed to the principles of individual liberty, democracy, human rights and the rule of law*", it presents NATO's three essential core tasks - collective defence, crisis management and cooperative security. It also emphasises Alliance solidarity, the importance of transatlantic consultation and the need to engage in a continuous process of reform. The document then describes the current security environment and identifies the capabilities and policies it will put into place to ensure that NATO's defence and deterrence, as well as crisis management abilities, are sufficiently well equipped to face today's threats. These threats include, for instance, the proliferation of ballistic missiles and nuclear weapons, terrorism, cyber attacks and fundamental environmental problems. The Strategic Concept also affirms how NATO aims to promote international security through cooperation. It will do this by reinforcing arms control, disarmament and non-proliferation efforts, emphasising NATO's open door policy for all European countries, and significantly enhancing its partnerships in the broad sense of the term. Additionally, it affirms that NATO will continue its reform and transformation process.

At the NATO Summit in Brussels (14 June 2021), leaders taked important decisions to chart the Alliance's course over the next decade. Allied leaders agreed on an ambitious NATO 2030 agenda to ensure the Alliance can face the challenges of today and tomorrow. They made decisions to strengthen political consultations, reinforce collective defense, enhance resilience, sharpen NATO's technological edge, uphold the rules-based international order, step up training and capacity building for partners, and address the security impact of climate change. They further agreed to develop NATO's next Strategic Concept for the summit in

2022. NATO leaders also agreed to a new cyber defense policy for NATO, and made it clear that the Alliance is determined to defend itself in space as effectively as in other military domains.

Why a new Strategic Concept? Because it is about the crafting of a new vision for the Alliance focusing on conceptual and policy issues that require clarification in the interest of re-establishing the strategic consensus.(Wittmann, 2009)

NATO's next Strategic Concept will help prepare the Alliance for a world of growing global competition and security threats. It will also recommit to the Alliance's founding values and enduring purpose, to safeguard the freedom and security of all Allies by political and military means.

The report *NATO 2030: united for a new era* (2020) states that "Allies must adopt a genuinely strategic mindset that goes beyond crisis-management."(NATO, 2020)

Regarding the US strategic options for the future of the security environment for 2035, the Joint Operating Environment 2035 (JOE 2035) is a document that describes the future security environment and projects the implications of change for the Common Force so that it can anticipate and prepare for potential conflicts. JOE 2035 illustrates some ideas on how changes in conflict and war could impact the capabilities and operational approaches required by the future Joint Force. Implications for the Joint Force are presented in section 3 of JOE 2035. (JOE 2035, 45). The United States will face a wide range of emerging – and often unforeseen – challenges in the future security environment featuring both *contested norms* and *persistent disorder*. Specific U.S. strategic and military objectives to address these challenges will be many, multi-faceted, and tailored to a specific time, place, and set of circumstances. However, the JOE relies on a range of strategic goals to describe the overall terms of national commitment and articulate an acceptable end state for any particular U.S. strategic endeavor. These are:

1. ***Adapt to changing conditions*** – ensure the United States can adequately cope with emerging changes in the security environment.
2. ***Manage antagonism and impose costs*** – discourage changes to the security environment that are unfavorable to the United States.
3. ***Punish aggression and rollback gains*** – block and undo changes to the security environment that are dangerous or disruptive to the United States.
4. ***Impose change and enforce outcomes*** – introduce desired changes to the security environment that are favorable to the United States.

This range of strategic goals suggests differing levels of engagement, commitment, or overall posture by the United States. Moreover, this range of goals represents a continuum and may change over time as a particular situation evolves. At the low end of this continuum, the United States might reactively manage security threats or otherwise respond to the consequences of natural and humanitarian disasters. At the high end, the United States might proactively solve a security problem by imposing a U.S. preferred solution that forces an adversary to accede to its will.

The role of the Joint Force to apply military power to support the achievement of strategic goals in concert with other elements of national power. To effectively pursue this range of goals, the Joint Force conducts four types of enduring military tasks against an array of competitors and in response to a range of phenomena. These are:

1. *Shape* or *contain* to assist the United States with coping and adapting to changed international security conditions.
2. *Deter* or *deny* to manage the antagonistic behavior of competitors or to impose costs on competitors or adversaries taking aggressive action.

3. *Disrupt* or *degrade* to punish aggressive action by an adversary or to force an adversary to retreat from previous gains.

4. *Compel* or *destroy* to impose desired changes to the international security environment and subsequently enforce those outcomes. (National Intelligence Council,2017)

The latest edition – Joint Operating Environment 2040 – was published in January 2020 and is the U.S. Joint Forces' most recent perspective on the future operating environment and the implications of that environment for Joint warfighting over the next two decades. The 2040 edition of the JOE differs from earlier versions in that it was written in a close and sustained partnership led by the Joint Staff J7, Defense Intelligence Agency (DIA), and the Joint Staff J2. It was strongly supported by Service futures organizations, including the Army's Mad Scientist Program, TRADOC G-2, and Army Futures Command. The new JOE is anchored in an "intelligence-driven, threat informed" view of the deep future. This approach reflects a new urgency to understand and address the growing threat of adapting great and regional power adversaries, as described in the most recent unclassified Summary of the National Defense Strategy (NDS), and to arrest – as then-Chairman Joseph Dunford put it – the erosion of our qualitative and quantitative military advantages. The first step in correcting our trajectory was to fully understand the problem from a Joint Force perspective. JOE 2040 – the first classified edition of the document – dives deeply into how the character of warfare is changing, how adversaries are addressing this change through novel ways of war, and the implications of both for the Joint Force.(Becker,2020)

5. Conclusions

Hybrid threats and hybrid warfare are real; they exist and define the current security environment. Combating hybrid threats is a challenging part of rethinking and redesigning security policy. Hybrid warfare can be defined as a complex combination of the following elements: parties involved, situations/events/conflict states, means, tactics and technologies used. There are views that hybrid threats influence decision-making at the local, regional, state or institutional level and deliberately target the vulnerabilities of states and democratic institutions. The classic/conventional war, known to most non-combatants, the war as a battle in a field between people and cars, the war as a massive decisive event in a dispute in international affairs, such a war no longer exists. The phrase "new war" introduces a new paradigm, namely that of "war between people", where all people, everywhere, are on the battlefield.

The challenges of hybrid warfare and hybrid threats are among the priorities of most governments around the world today. Hybrid warfare is a style of warfare in which victory allows and demands whatever means will be successful: the ethics of total warfare applies to even the smallest fight.

The concepts of "hybrid threats" and "hybrid warfare" have gained increasing prevalence in the analysis of the contemporary security environment. The revisionist powers, facing a rising NATO and a hyper-powerful United States in the post-war era, have discovered how to confront the West on the verge of "use of force" or "armed attack," as stated in the Charter of the United Nations. In view of the major changes that have taken place in the last two or three decades in the global security environment, NATO and the USA make major efforts to adapt but also apply a proactive strategy to prevent and deter possible hybrid threats.

References:

1. Balaban, M. & Mielniczek, P., 2018, *Hybrid conflict modeling*, DOI: 10.1109/WSC.2018.8632492, https://ieeexplore.ieee.org/document/8632492
2. Becker, J., 2020, *Joint Operating Environment 2040*. Retrieved from https://madsciblog.tradoc.army.mil/291-joint-operating-environment-2040/
3. Cullen, P. et al., 2021, *The landscape of Hybrid Threats: A Conceptual Model*. Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305
4. European Commission, 2016, *EU operational protocol for countering hybrid threats,* https://www.statewatch.org/media/documents/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf
5. European Commission, 2021, *Hybrid CoE, Hybrid threats as a concept,* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
6. Gressel, G., 2019, *Protecting Europe Against Hybrid Threats*, https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf
7. Kamp, K.-H., 2016, *Why NATO Needs a New Strategic Concept*, NATO Defense College, https://www.ndc.nato.int/news/news.php?icode=997
8. Marcuzzi, S., 2018, *Hybrid warfare in historical perspectives*. Retrieved from http://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf
9. National Intelligence Council, 2017, *Global Trends: Paradox of Progress.* www.dni.gov/nic/globaltrends, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf
10. NATO, 2020, *NATO's Political Purpose in the 21st Century, in NATO 2030: united for a new era.* https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf
11. Rühle, M.& Roberts, C., 2021, *Doter l'OTAN de nouveaux outils de lutte contre les menaces hybrides,* https://www.nato.int/docu/review/fr/articles/2021/03/19/doter-lotan-de-nouveaux-outils-de-lutte-contre-les-menaces-hybrides/index.html
12. Schmid, J., 1990, *Der Archetypus hybrider Hybride Kriegfuhrung vs.militarisch zentrierte Kriegfuhrung*, https://www.oemz-online.at/pages/viewpage.action?pageId=43614262
13. Tenenbaum, E., 2015, *Hybrid Warfare in the Strategic Spectrum: An Historical Assessment*, in *NATOs response to hybrid threats*, 102, NATO Defense College, Forum Paper 24, Edited by Guillame Lasconjarias and Jeffrey A.Larsen, 2015, Rome, Italy. https://stratcomcoe.org/cuploads/pfiles/2nd_book_short_digi_pdf.pdf
14. TRADOC, 2015, *The Operational Environment, 2035-2050: The Emerging Character of Warfare.* https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/217736
15. Weissmann, M., 2019, *Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework*, Journal on Baltic Security https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC_2_23829230%20-

%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20and%20hybrid%20threats%20today%20and%20tomorrow_%20towards%20an%20analytical%20framework.pdf

16. Wittmann, K., 2009, *Towards a new Strategic Concept for NATO*. NATO Defense College, Forum Paper 10, Rome, Italy. https://www.files.ethz.ch/isn/108701/fp_10.pdf