Bulletin of "Carol I" National Defence University
10.12753/2284-9378-20-22

THE INTEGRATED APPROACH – CONSIDERATIONS, POTENTIAL, AND LIMITATIONS

Maj. Dumitru GEORGESCU, PhD Candidate*

The current security environment is characterized by complex challenges. The emergence of hybrid threats has determined an increase in the complexity and ambiguity of the operational environment. In order to cope with these security challenges, it is necessary to synchronize the application of the instruments of power. Therefore, it is imperative to conceptualize and operationalize an integrated approach. The solving of the wicked problem of hybrid threats can be facilitated by an integrated approach.

Keywords: security environment; hybrid threat; integrated approach; comprehensive approach; security.

The contemporary operating environment is characterized by complexity, volatility, uncertainty, and ambiguity[1]. Complexity is the result of the large number of actors and systems that operate in the environment, as well as the numerous relationships and inter-dependencies between them. Volatility is determined by the environment instability, which manifests itself in often and significant changes. Uncertainty is caused by the lack of predictability and ability to anticipate the direction or moment of changes that occur. Ambiguity, the most relevant characteristic when the need of using an integrated approach is discussed, is generated by the lack of clarity in identifying cause-effect relationships[2]. Where ambiguity is concerned, multiple actors can have multiple opinions as to what causes a particular effect. Although these effects are perceived in similar ways, their causes may be identified as different. The relevant solution obtained by adding different perspectives is probably the most realistic one.

In this context, The Strategic Concept for the defence and Security of the Members of the North Atlantic Treaty Organization has revealed the need to adopt a comprehensive approach to effectively manage crisis situations. The document, signed by the highest officials of NATO states at the Lisbon Summit in November 2010, recognizes the necessity and defines the transition from relatively isolated application of the military instrument to a more comprehensive framework, where it can be applied together with the other instruments of power. The lessons learned from NATO operations, especially the ones in Afghanistan and the Balkans, have shown that a comprehensive approach in what concerns political, civilian and military domains is needed for efficient crisis management. In this context, the Alliance is going to get actively involved, together with other international actors, before, during and after crisis situations, in order to encourage analysis, planning and conducting the activities and actions in the field in a collaborative manner, at the same time being aware of the coherence and efficacy degree of the entire international effort[3]. This approach was generated by the need to address an ever-growing array of challenges of the local and global security and stability.

**Ministry Of National Defence*
e-mail: *dumitru.i.georgescu@gmail.com*

Threats to security

A conventional threat, as defined by the probability of a traditional military attack on territories of member states, although very small, is not to be neglected. In the context of the recent significant technological development, advanced military capabilities have been developed and are now available. The risk of using such capabilities cannot be ignored, as it can have serious consequences, difficult to anticipate and manage. The intention of some state actors to exert their domination at a regional and global level, by developing nuclear and mass destruction weapons presents a continuous challenge and makes the military instrument even more relevant than ever[4].

Conventional threats are completed by new challenges to the security of the states, such as terrorism, instability and conflicts at the NATO

borders and beyond. Cyber threats, organized crime and their cross-border activities (weapons, narcotics and person trafficking) are added to the challenges that member states face, thus calling for a comprehensive approach to common defence through deterrence, prevention and management of crises, as well as promoting security through cooperation.

The emergence of hybrid war, as a way to synchronize the use of power instruments adapted to exploit specific vulnerabilities across the societal functions in order to obtain synergistic effects[5], determines a greater complexity and ambiguity in the current operating environment. Actions specific to this type of threat are usually characterized by a low level of attribution (they cannot be associated with the aggressor) and a low level of intensity (they cannot be detected by the target's systems). The dynamic and complex sum of threats results in multiple actions, synchronized or not, the cause interrelating effects. Figure 1 shows a representation

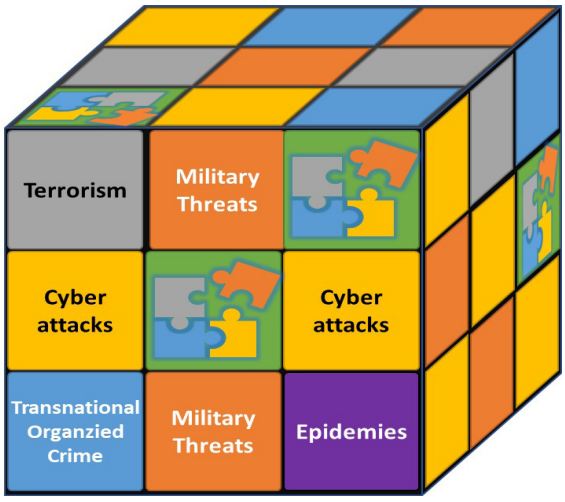

Figure 1 *Threats specific to the contemporary security environment*

of the current security environment specific threats. Ensuring security in the present operational environment is the same as managing a complex mix of threats – military, hybrid, cyber-attacks, pandemics, terrorism and organized crime.

The comprehensive approach – conceptual origin of the integrated approach to security in the context of hybrid threats

In order to implement the NATO strategic concept approved in November 2010, The Comprehensive Operational Planning Directive was developed. This directive mentions four instruments of power – military, political, economic and civilian. The military instrument refers to the application of military strength, to include threat or use of lethal or non-lethal force in order to deter, constrain or defeat an adversary, by disrupting or destroying his critical military or non-military capabilities. The political instrument includes use of political means, especially diplomatic ones, to cooperate with different actors in order to influence adversaries, or to create advantageous conditions. The economic instrument includes initiatives, incentives or sanctions that can be applied to the money or services flow, as well as financial support for state or non-state actors in crisis. The civilian instrument includes domains such as justice, public order and law enforcement, education, public communication and infrastructure that enables access to basic services (health, food, power, water)[6].

American doctrine mentions four instruments of power – diplomacy, information, military and economics, which are referred to as DIME. Diplomacy is about interactions with state or non-state actors in order to reach some agreements and accords that would allow the parts to function together, in spite of divergent interests. Information includes creating, exploiting and – in particular situations – disrupting knowledge. By using this instrument, a state intends to protect its own ability to collect and use information, as well as to diminish or disrupt the adversary's same ability. The military instrument includes the threat of force, use of force or facilitating the use of force by another party in order to promote a state's own interests. Economics concentrates on promoting or disrupting the ability to have a stable, prosperous climate[7]. Although DIME has described the instruments of national power in the American vision for some time, there is a tendency to further granulate the options policy makers have at their disposal. Therefore, by introducing domains such as financial, law, intelligence, and development, DIME has turned into MIDFIELD[8]. As a result, the instruments of national power become more focused.

In order to analyze the comprehensive approach from NATO and European Union (EU) perspective, as well as to describe the integrated approach to security, we will use a set of five characteristics: multi-instrumental, multi-phased, multi-level, multilateral and multi-*directional*. Four of these characteristics come from the EU vision on the

integrated approach, the fifth has been added to address the particularities of the hybrid threat manifestation.

The Global Strategy for External and Security Policy of the European Union (EU) states what the characteristics of an integrated approach are for this organization. In EU's vision, the integrated approach is multi-*dimensional*, multi-phased, multi-level, and multilateral. The multi-dimensional approach means using all the policies and instruments available to the EU in order to prevent, manage and put an end to conflicts. The multi-phased characteristic refers to the involvement in all the phases of the conflict – prevention, ending, stabilization. The multi-level characteristic means acting at local, national, regional and global levels to manage conflicts. Multi-laterality refers to engaging all the actors involved in the conflict or those have a role in ending it[9]. In order to highlight the synchronized application of a state's instruments of power specific to this approach, this article will use the term multi-instrumental, as opposed to multi-dimensional. This inversion of terms will also help avoid a potential confusion, caused by the multi-dimensionality of the operational environment components. We will also introduce the term multi-directional, to highlight the necessity to adopt an integrated approach that will be appropriate to address the numerous threats in the contemporary security environment.

NATO vision on implementing the comprehensive approach includes keeping track of the contribution of all relevant actors of the operating environment to crises management efforts, based on a common goal, collective responsibility, openness and determination. Implementing the comprehensive approach to managing crisis situations is facilitated by interactions between civilians and the military at all levels of the military institutions. At a political and strategic level, the important aspect is building tighter connections and relations with relevant actors, without affecting their ability to autonomously make decisions. At an operational level, cooperation between international actors, both regional and local, is a priority for planning operations. At a tactical level, the allied forces commanders will effectively cooperate and coordinate with local and international actors and authorities, to conduct military operations[10].

This approach has, therefore, a multi-instrumental characteristic, where the role of the military instrument is the most important. This generates a slight limitation on multi-instrumentality. Implementing military art at all levels underlines the multilevel characteristic of the comprehensive approach defined by NATO. By working to involve all relevant actors in crisis management, it ensures the multi-laterality of this approach. Although the comprehensive approach intends to harmonize efforts of all relevant actors, this is very difficult to do. Therefore, multi-laterality is limited. Since the comprehensive approach addresses all phases of a crisis or a conventional military threat, it can be defined as multi-phased. However, NATO cannot actively respond to the entire spectrum of threats on security. Therefore, the multi-directional characteristic of this approach is reduced.

The Global Strategy for EU External and Security Policy adopted in 2016 mentions for the first time the concept of an integrated approach, conceptually substantiated by the four characteristics described above. Therefore, the comprehensive approach is the origin of the integrated approach concept. In the context of the contemporary security environment and especially that of hybrid threats, it is imperative to transition from a comprehensive approach to an integrated one, at least at a national level. In order to fight actions related to hybrid threats, that have effects in multiple dimensions of the operating environment, it is necessary to apply the instruments of state power in a synchronized manner, in all components and dimensions of the operating environment.

The integrated approach to security in the context of hybrid threats

In order to conceptualize an integrated approach, it is necessary to adopt a set of state power instruments. We will consider five instruments for the following model – military, economic, diplomatic, information, and civil – MEDIC. The integrated approach to security means the application of these instruments of power in order to achieve the objectives that fulfill the security interests. The integrated approach is based, therefore, on the existence of a single purpose – ensuring national security. This objective is a priority in a context in which the primary responsibility to address hybrid threats goes to the target nation. Still, NATO is ready to assist any member state when it comes to

fighting hybrid threats[11]. It is, therefore, necessary to use an approach to security that will identify the manifestations of hybrid threats and ensure a proper initial response. In order for this to be possible, considering the particularities of hybrid threats, integrating the power instruments is paramount.

The synchronized application of the instruments of power offers benefits in promoting security interests. The operating environment is characterized by multiple components and dimensions. In order to understand it, a systemic perspective can be adopted. According to this, the relevant actors, no matter their affiliation – allied, neutral or opposing – are seen as systems. A system is defined as a group of elements that normally interact or are inter-dependent, being related based on functions or behaviors, and constitute a whole. These systems consist in links and nodes. The nodes represent the elements inside the system. They belong to different components and dimensions of the operating environment. Links are the connections between the nodes of the same system or of different systems. These represent the way nodes interact and are inter-related. Links can be technical, human, social, functional, organizational, any kind of connection between nodes.

The multi-instrumental characteristic of the integrated approach refers to the possibility to understand the links between nodes of different operational environment components and dimensions. In this context, we can correctly identify any situation specifics and act according, efficiently and effectively, on the critical nodes, in order to modify the system behavior in the desired direction. This multi-instrumental characteristic makes it possible to identify vulnerabilities belonging to both the adversary and to our own system. By protecting our system's vulnerabilities, especially in the context of hybrid threats, we ensure the necessary resilience. By targeting the vulnerabilities of adversaries who use hybrid war, we create the conditions to defeat them and ensure local, national or global security.

The multilateral characteristic of the integrated approach consists in establishing a wide variety of links between different actors, relevant within the context of promoting the national security interests. The typology of the links between these actors is defined by the level of interactions. This level is dynamic and will evolve while dealing with security challenges.

These levels are: coexistence, consultation, deconflicting, coordination, cooperation[12], and collaboration. Coexistence represents the simultaneous existence of several things, beings, phenomena[13]. The actors exist in the same space-time frame, with no direct interaction. Consultation is a limited interaction, in order to exchange opinions or ideas between coexisting actors. Deconflicting is the interaction between two actors, with the purpose of avoiding unwanted interferences of one's actions over the other. Coordination is defined as having all parts of a whole agree on something, guiding a series of activities to achieve the same goal[14]. Coordination is meant to make the relationship between actors efficient, by contributing different elements to complex activities. Most often, cooperation is achieved by exchanging information. Cooperation is defined as different entities working together[15].

In addition to coordination, actors work in a common manner to achieve mutual benefits. Although their objectives are different, fragments of these can be attained by common action. Responsibilities remain different. Collaboration means participating alongside other entities to achieve something that is being worked on in common[16]. This type of relationship is based on common objectives of different actors. In order to achieve the common objectives, they contribute information and resources, and they share responsibilities. The integration of the interaction, as well as the complexity of the relationships between actors are greater as these interactions levels grow, as presented in Figure 2.

The multi-laterality of the integrated approach must be understood in relation to the multi-level characteristic. The integration and the complexity of the interaction levels manifest themselves between relevant allied and neutral actors, at a global, regional, national and local level, thus resulting a multiplication of the way different levels of interaction manifest themselves. If, on a global level, two actors can coexist, on a local level, in order to manage a crisis, they can consult or deconflict actions, at least in what concerns space and time.

The multi-directional attribute of the integrated approach represents its capacity to respond adequately and timely to all threats in the security

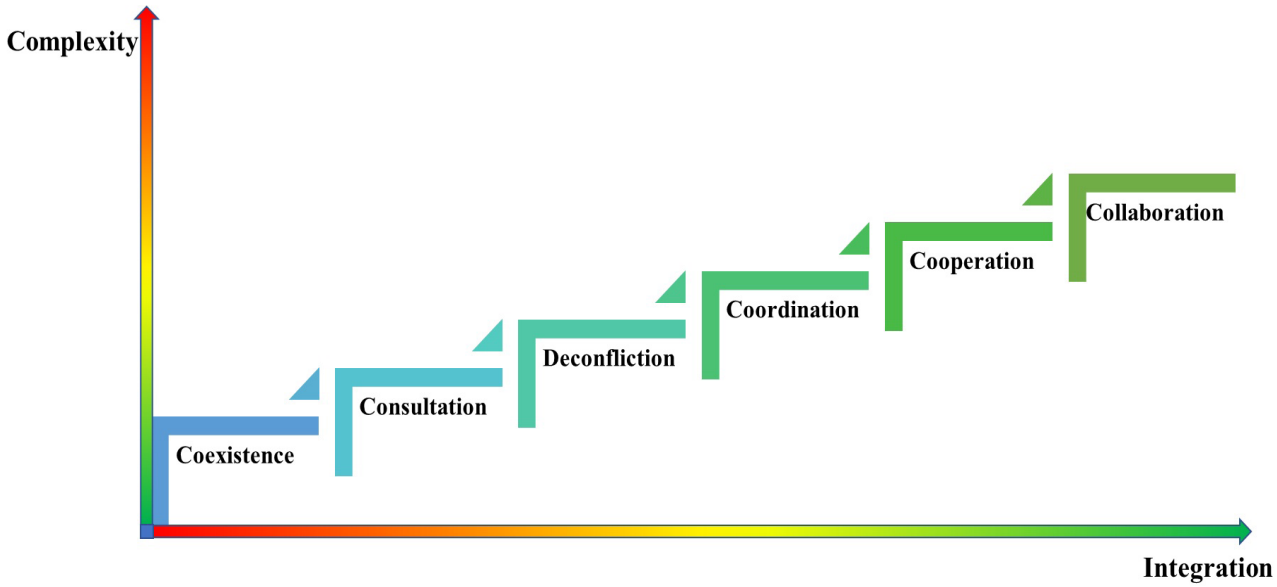

Figure 2 *Levels of interaction among actors*

environment. Military or non-military threats can manifest individually or as dimensions of a hybrid threat. By using an integrated approach, we can lower the detection threshold of the threat, as a result of easier identification of the source and cause of its actions and effects, in all domains of the operational environment. This way, it becomes possible to identify threats that are isolated, un-synchronized or synchronized as a part of a hybrid war waged by an aggressor.

The multi-phased characteristic of the integrated approach facilitates the synchronized application of power instruments at the very early stages of a threat manifesting itself. This way, not only can crises or actions related to different challenges to the security situation can be detected early on, but it offers the possibility to prevent, contain or deter such circumstances. This will allow for an effective and efficient response, by cutting operational costs.

Conceptualization of the integrated approach is ensured by its defining characteristics – multi-instrumental, multi-level, multilateral, multi-phased and multi-directional. In order to create a collaborative framework to allow implementation of this concept, procedural, technical, actional and cognitive measures need to be taken. The technical infrastructure must facilitate information exchange between actors, using safe channels, with minimal operational costs, and has to allow the implementation of the procedural and technical framework that is needed for the integrated approach. Therefore, on a cognitive level, accepting the ambiguity and complexity of the operational environment as well as proving a sufficient level of mutual trust are necessary conditions, in addition to the technical, procedural and actional ones. No matter the type of the threat, the complexity, volatility, ambiguity and uncertainty of the operational environment make the transition to an integrated approach necessary.

Synchronizing how instruments of power (MEDIC) are applied, is the foundation of the integrated approach. The degree of synchronization of the military, economic, diplomatic, information and civil instruments depends on the following factors: the levels at which they are synchronized, the phase of crisis management and threat neutralization, as well as the way in which actors in the operational environment and their connections are perceived. At the same time, the omni-directional ability of the sensors belonging to actors to identify actions specific to different threats ensure an operationalization of the integrated approach.

The potential of an integrated approach

Hybrid threats have caused a lot of concern to international and national security institutions. Hybrid threats are different from others in nature and manifestation. The first challenge in managing hybrid threats is detecting them. In order to ensure an effective and efficient response of power instruments, it is necessary to identify a manifestation of such a threat in its early phases. In other words, in order to neutralize such a threat, it is necessary to be warned against its manifestation

in a timely manner, so that a proper response is planned and implemented. This concept is defined as early warning, by extending the initial definition – early notification of launching or approaching weapons or weapons carriers[17]. Based on early warning of a hybrid threat manifestation, an entity may contain the effects of initial actions, deter further actions and, eventually, defeat the aggressor that uses hybrid warfare to promote its own security interests.

Although early warning for hybrid threats is necessary, it is very difficult to obtain. One of the fundamental characteristics of these threats is that early warning in this case is not an easy task. This relative weakness in diagnosing political and economic indicators that lead to multiple directions possibly associated with a threat is a very important problem that must be solved[18].

There are currently state actors that have capabilities and resources that considerably surpass those of terrorist organizations, and have proven their willingness and intention to project hybrid threats to include non-kinetic means and capabilities in order to affect democratic states' vulnerabilities. By increasing ambiguity, evasiveness and using actions under the detection threshold of the target state, by engaging non-military instruments to attack society in its entirety, hybrid threats represent a new form of complexity[19].

Maintaining actions that represent a hybrid threat means acting in a way that can be defined by two characteristics: a very low level of attribution and performing actions under the detection threshold of the target state. These two coordinates ensure the element of surprise in relation to the institutions that are tasked with achieving and maintaining security.

Achieving a low level of attribution not only causes difficulties in detecting actions associated with hybrid war, but also ensures plausible denial and delimitation from such actions of an aggressor. In this context, the international bodies that ensure security have difficulties in acting in response to punish the aggressor.

There are different ways to achieve a low level of attribution. One way is to use an actor that is not affiliated with the aggressor as the source of the action. To this purpose, one can use different actors, such as non-governmental organizations, companies, extremist political parties, or radicalized factions of different groups. The connection to these source actors is very difficult to identify by a conventional approach to security. Another way that a hybrid aggressor can achieve a low level of attribution is by using direct and potential influences between operational environment variables.

In order to act below the detection threshold of the target state, in addition to using direct and potential influences, the aggressor can perform smaller-scale actions in different variables of the operational environment. They will help achieve desired effects by creating synergy. Instead of vertically escalating the intensity of actions, the aggressor will use a horizontal escalation throughout the operational variables, thus targeting the lack of integration in power instruments[20] – MEDIC.

Conceptually the integrated approach is multi-instrumental, multi-level and multilateral. Its multi-instrumental characteristic ensures integration of all instruments of power. This way, we can simultaneously monitor specific detection thresholds for every instrument. Therefore, we can identify actions that are over the detection threshold specific to each instrument – military, economic, diplomatic, information or civil.

The multi-level attribute of the integrated approach ensures the integration of power instruments at all levels – local, national, even regional or global. This way, the detection threshold for each instrument can be lowered. This should be achieved in a controlled manner, across all instruments of power. The potential result of the multi-instrumental and multi-level characteristics of the integrated approach is a detection ability that will identify isolated actions as part of a hybrid threat.

In the absence of multi-direction, the instruments act in a synchronized manner at all levels, but they only identify actions specific to each domain. As an example, in this context, there is a chance that a part of the economic dimension of a hybrid threat will not be identified by the economic instrument of power, but by the others. In a multidirectional situation, their integration is facilitated and the action will correctly be identified as part of a hybrid threat.

Separately, the three characteristics described above cannot solve the issue of low attribution. The major contribution in this domain comes from the multilateral characteristic of the integrated approach.

It facilitates a perspective from all the actors, no matter the variable of the operational environment they act in. The connections can be identified by common knowledge among the instruments of power, which will lead to understanding of the hybrid threat, in terms of existence and size of its manifestation. All these dimensions lead to the multi-phased attribute of the integrated approach.

The aspects presented above indicate that the integrated approach has the potential to identify the manifestation of a hybrid threat and to ensure early warning. At the same time, by offering the possibility to synchronize capabilities from different instruments of power, or to deploy groups of such capabilities especially designed to this purpose, the integrated approach offers the framework to timely and adequately manage security challenges posed by hybrid threats.

Limitations of the integrated approach

However, identifying the manifestation of a hybrid threat and early warning constitutes a wicked problem[21]. Wicked problems present ten specific traits:

- they cannot be definitively formulated. Wicked problems cannot be formulated so that they can offer to a person trying to solve them the necessary data for that endeavor. When one tries to define them, the definition depends largely on the idea used to solve them;
- they do not allow definitive solutions. Finalizing efforts to solve them is not a consequence of success, but rather of reaching an acceptable level or investing more resources, time or effort than was originally planned for solving the problem;
- they do not have true or false solutions. The attempts to solve these problems can be better, worse, or satisfactory;
- there is no way to immediately or definitely evaluate a solution. There is a possibility that some of the actions used to solve the problem may have worse consequences than the things they were trying to solve;
- each action done to solve the problem has consequences. Each change in a decision potentially generates other wicked problems;
- they do not have a set of potential solutions or a set of allowed operations. Courses of action are determined by the capacity to judge in a realistic manner, the mindset to accept out-of-the-box ideas and the degree of trust that exists among those trying to solve the problem;
- they are unique. There may be similarities between two wicked problems, but the differences will determine that similar courses of action used to solve them to not necessarily be successful;
- each wicked problem can be considered a symptom of another wicked problem;
- discrepancies associated with these problems can be explained in numerous ways. Choosing one explanation determines the approach used to solve the problem;
- those trying to solve wicked problems need to understand that the hypotheses they formulate will not be confirmed, but rather the inadequate hypotheses will be proven wrong[22].

In this light, trying to identify and have early warning on a manifestation of hybrid threats seems inadequate and deemed a sure failure. Obviously, such a challenge is difficult to solve. This exact difficulty gives its operational value and is the reason for which aggressors resort to hybrid warfare. The integrated approach cannot guarantee a definitive and universal solution to ensure security, where hybrid threats are concerned. What is does offer is the framework for identifying them, limiting and containing their effects, as well as deterring future actions by reducing the benefits and increasing operational costs for the aggressor.

Conclusion

As highlighted above, the integrated approach is necessary in the context of hybrid threats. Unfortunately, none of the implementation possibilities can be surely described as the best way to solve security challenges posed by hybrid warfare. The possible solution is influenced by vulnerabilities in the society, the possibilities of the states, the organizational culture of the power instruments and by the aggressor's particularities, capabilities, resources, and objectives.

The integrated approach cannot offer a universal solution to such a challenge. It is not an operational silver bullet. It cannot offer all the answers and cannot guarantee success in managing the hybrid threat.

Its value resides in its potential to identify and manage the manifestation of hybrid threats. If we were to match the integrated approach against one of the wicked problems characteristics, it is the last

one that describes it the best. This approach cannot be confirmed as a valid hypothesis, but it is the least probable to be proven wrong.

NOTES:

1 [Stiehm, Judith Hicks; Townsend, Nicholas W.], *The U.S. Army War College: Military Education in a Democracy*, Temple University Press, 2002, p. 6.

2 https://hbr.org/resources/images/article_assets/hbr/1401/F1401C_A_LG.gif, accessed on 05/15/2020.

3 [North Atlantic Treaty Organization], NATO, *Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, 2010, p. 19.

4 *Ibidem*, p. 10.

5 Patrick J. Cullen, Erik Reichborn-Kjennerud, *Multinational capability development Campaign Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, 2017, p. 8.

6 [Supreme Headquarters Allied Powers Europe], NATO, *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim V2.0*, 2013, p. 1-9.

7 [Joint Chiefs of Staff], USA, *Joint Doctrine Note 1-18, Strategy*, 2018, pp. II-5–II -56.

8 [Joint Chiefs of Staff], USA, *Joint Doctrine Note 1-18, Strategy*, 2018, p. vii.

9 [EU], *Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union's Foreign and Security Policy*, 2016, pp. 28-29.

10 [North Atlantic Treaty Organization], NATO, *AJP-01 Allied Joint Doctrine Edition E Version 1*, NATO Standardization Office, 2017, pp. 2-4.

11 https://www.nato.int/cps/en/natohq/topics_156338.htm, accessed on 05.15.2020.

12 https://www.handbook.cimic-coe.org/1.introduction/1.1nato-and-a-comprehensive-approach/, accessed on 05.01.2020.

13 https://www.dex, accessed on 05.01.2020.

14 *Ibidem*.

15 *Ibidem*.

16 *Ibidem.*

17 [NATO], *AAP-06 Edition 2019, NATO Glossary of Terms and Definitions (English and French)*, NATO Standardization Office, p. 46.

18 Patrick Cullen, *Hybrid threats as a new "wicked problem" for early warning*, Hybrid Centre of Excellence, 2018, p. 5.

19 *Ibidem.*

20 Patrick J. Cullen, Erik Reichborn-Kjennerud, *Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, Multinational Capability Development Campaign, 2017, p. 8.

21 Patrick Cullen, *op.cit.*, p. 5.

22 Horst W. J. Rittel, *Dilemmas in a General Theory of Planning*, Policy Sciences, 4:2, pp. 161-167.

REFERENCES

[Department of the Army], *Army Doctrine Publication No. 2-0, ADP 2-0, Intelligence*, USA, July 2019.

[Department of the Army], *Army Doctrine Publication No. 3-0, ADP 3-0, Operations*, USA, July 2019.

[Department of the Army], *Army Doctrine Publication No. 5-0, ADP 5-0, The Operations Process*, USA July 2019.

[Department of the Army], *FM 6-0 Commander and Staff Organization and Operations*, USA, May 2014.

[EU], *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*, 2016.

[Joint Chiefs of Staff], *Joint Doctrine Note 1-18, Strategy*, USA, 2018.

[Joint Chiefs of Staff], *Joint Concept for Operating in the Information Environment (JCOIE)*, USA, July 2018.

[Joint Chiefs of Staff], *Joint Publication 2-0, Joint Intelligence*, USA, October 2013.

[Joint Chiefs of Staff], *Joint Publication 2-01, Joint and National Intelligence Support to Military Operations*, USA, July 2017.

[Joint Chiefs of Staff], *Joint Publication 2-01.3, Joint Intelligence Preparation of the Operational Environment*, USA, May 2014.

[Joint Chiefs of Staff], *Joint Publication 3-0, Joint Operations*, USA, October 2018.

[Joint Chiefs of Staff], *Joint Publication 3-08, Interorganizational Cooperation*, USA, October 2016.

[Joint Chiefs of Staff], *Joint Publication 3-24, Counterinsurgency*, USA, April 2018.

[Joint Chiefs of Staff], *Joint Publication 5-0, Joint Planning*, USA, July 2018.

[Land Warfare Development Centre], *Army Doctrine Publication Land Operations*, UK, March 2017.

[North Atlantic Treaty Organization], *Active Engagement, Modern Defence - Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, 2010.

[North Atlantic Treaty Organization], *Allied Joint Publication 01, AJP-01, Allied Joint Doctrine*, February 2017.

[NATO], *AAP-06, NATO Glossary of Terms and Definitions (English and French)*, NATO Standardization Office, 2019.

[Supreme Headquarters Allied Powers Europe], NATO, *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim V2.0*, 2013.

[Supreme Headquarters Allied Powers Europe], NATO, *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim V2.0*, October 2013.

Cullen J. Patrick, Reichborn-Kjennerud Erik, *Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, Multinational Capability Development Campaign, 2017.

Cullen Patrick, *Hybrid threats as a new "wicked problem" for early warning*, Hybrid Centre of Excellence, 2018.

Rittel Horst W.J., "Dilemmas in a General Theory of Planning", *Policy Sciences*, 4:2.

Stiehm Judith Hicks, Townsend Nicholas W., *The U.S. Army War College: Military Education in a Democracy*, Temple University Press, 2002.

https:// www.hbr.org/resources/images/article_assets/hbr/1401/F1401C_A_LG.gif

https://www.nato.int/cps/en/natohq/topics_156338.htm

https://www.handbook.cimic-coe.org/1.introduction/1.1nato-and-a-comprehensive-approach/

https://www.dex.ro/