IX INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023" -
29th and 30th September 2023, Belgrade, Republic of Serbia

TOOLS TO REDUCE VULNERABILITY FROM HYBRID THREATS

Tatjana Gerginova[1]
[1] University "Sv. Kliment Ohridski" Bitola, Faculty of Security Skopje, Republic of North Macedonia, tatjana.gerginova@uklo.edu.mk

Received: 3th July 2023
Accepted: 4th August 2023

Professional paper

Abstract: *Building national resilience is the primary responsibility of member states because countering hybrid threats relates to national security and defense. However, today many member states face common threats that can be effectively addressed at the level of the European Union. In the paper, the author analyzes the need – to combine European and national instruments in building the resistance of the member states to hybrid threats and in preventing, reacting and recovering from the crisis. In the final part, the author analyzes the instruments whose application is aimed at creating the ability to detect and reduce vulnerability from hybrid threats in order to increase the ability to respond. In the concluding observations, the author gives recommendations in the direction of how each national country can efficiently and effectively deal with hybrid threats (Establishing cooperation with EU and NATO institutions, intended to deal with hybrid threats; the complexity of hybrid threats requires the full involvement of all institutional stakeholders in the national security system; Promotion of cooperation and exchange of information at the national and international level; Building high-quality and trained key personnel, as well as maintaining the basic principles of national security and resilience of society through constant basic training).*

Key words: *hybrid threats, building resilience, hybrid threats vulnerability*

1. INTRODUCTION

In recent years, the security environment of the European Union has been changing dramatically. Many of the current challenges to peace, security and prosperity stem from instability in the EU's immediate neighborhood and the changing forms of threats. They have an impact on the internal and external security of the EU. Today, many member states face common threats that can be more effectively addressed at the level of the European Union. The European Union can be used as a platform to strengthen national efforts and through its regulatory capacity, establish common benchmarks that can help raise the level of protection and resilience across the EU. The EU can therefore play an important role in improving our collective situational awareness, in building Member States' resilience to hybrid threats and in crisis prevention, response and recovery.

2. HYBRID THREATS AS A CONCEPT

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 (Hybrid CoE, 2022).

By using the aforementioned unconventional and conventional means in concert, hybrid actors conceal their action. The use of different intermediaries – supports the achievement of these goals. A hybrid action is cost-effective because it turns the vulnerabilities of the target into a direct strength for the hybrid actor. This makes hybrid action more difficult to prevent or respond to. The ongoing transition in international power structures provides a fertile environment for hybrid action. The intensifying conflict of values between the West and authoritarian states erodes international norms and institutions and makes open Western societies targets of comprehensive hybrid action. A conflict of values that extends to the domestic sphere of Western societies increases polarization and disunity within and among Western actors, making them more vulnerable to external interference. Recent developments in modern technology and an increasingly complex information environment provide powerful instruments for hybrid actors if not properly countered by the Western community.

Accordingly, Hybrid CoE characterizes hybrid threats as: (Hybrid CoE, 2022), (Steingartner & Galinec, 2021).

- 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 fulfill the agent's strategic goals while undermining and/or hurting the target (Available at https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/)

3. A COMMON FRAMEWORK FOR DEALING WITH HYBRID THREATS

During 2015, the European Commission and the High Representative adopted a Common Framework for Countering Hybrid Threats and Fostering the Resilience of the European Union, its Member States and Partner Countries, while increasing cooperation with NATO to counter these threats (See more: http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm - https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250).

The Joint Framework offers a comprehensive approach to improve the common response to the challenges posed by hybrid threats to Member States, citizens and the collective security of Europe. It brings together all relevant actors, policies and instruments to both counter and mitigate the impact of hybrid threats in a more coordinated manner. In particular, it builds on the European Agenda on Security adopted by the Commission in April 2015, as well as on

sectorial strategies such as EU Cyber Security Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy. Together with the upcoming European Union Global Strategy for foreign and security policy and the Defense Action Plan, and ongoing work on capacity building in support of security and development (CBSD) in third countries, the Joint Framework is part of the strategy of the Commission and the High Representative to increase the EU's capacity as a security provider.

The Joint Framework brings together existing policies and proposes twenty-two operational Actions aimed at:

- *raising awareness* by establishing dedicated mechanisms for the exchange of information between Member States and by coordinating EU actions to deliver strategic communication;

- *building resilience* by addressing potential strategic and critical sectors such as cyber security, critical infrastructures (Energy, Transport, Space), protection of the financial system from illicit use, protection of public health, and supporting efforts to counter violent extremism and radicalization;

- *preventing, responding to crisis and recovering* by defining effective procedures to follow, but also by examining the feasibility of applying the Solidarity Clause (Article 222 TFEU) and the mutual defense clause (Art. 42(7) TEU), in case a wide-ranging and serious hybrid attack occurs;

- stepping up the cooperation and coordination between the EU and NATO as well as other partner organizations, in common efforts to counter hybrid threats, while respecting the principles of inclusiveness and autonomy of each organization's decision making process.

The Framework is designed to provide a robust foundation to support Member States in countering hybrid threats collectively, supported by a wide range of EU instruments and initiatives.

The Joint Framework outlines proposals to build resilience in areas such as cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. In each of these areas, the implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation is a key first step, while some more concrete proposals have been put forward to further reinforce these efforts. The Joint Framework addresses the challenges raised by the specificities of threats of a hybrid nature, but EU action is not limited to countering hybrid threats. EU internal policies already aim at increased resilience and prevention, and at a rapid and effective response to crisis.

4. A BASIS FOR BUILDING RESILIENCE AND DEALING WITH HYBRID THREATS IN THE REPUBLIC OF NORTH MACEDONIA

In the Republic of North Macedonia, a Strategy for building resilience and dealing with hybrid threats has been adopted (According to https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf accessed on 15.05.2023).

The goal of this strategy is to create national resilience, as well as efficiently and effectively deal with hybrid threats. To achieve this goal, the Strategy is aimed at creating the ability to detect and reduce vulnerability from hybrid threats while seeking to increase the ability to respond, in accordance with the framework established by NATO and the EU. The activities of the state will be divided into six areas of operational activities.

During 2016, the faces new pressures such as population growth, urbanization, land and eco-systems' degradation, the lack of natural resources, fragility of states and complex conflicts. Hence the need to build resilience. Resilience is the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development (Available at https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf).

Resilience can be built at various levels. The notion of the resilience of NATO member states through maintaining and developing their individual and collective defense capacity is rooted in the Alliance's 1949 Founding Treaty. This is, in particular, established in Article 3 where the internal dimension of resilience is implicitly defined in terms of capabilities and the capacity for collective defense is operational zed through NATO's defense planning and capability development process. NATO defines resilience as "a society's ability to resist and recover from such shocks" as natural disaster, failure of critical infrastructure, or a hybrid or armed attack (According to "Resilience and Article 3", NATO, 2021).

This definition touches on two features of resilience: First, resilience concerns the ability to absorb and recover from a state of crisis (Ben Caves et al., 2021).

Second, resilient actors must be able to respond to a range of potential shocks, both expected and unexpected. This relates to the ability to survive; as one widely adopted definition of resilience puts it, an actor must be able "to maintain its core purpose … in the face of dramatically changed circumstances" (Andrew Zolli and Ann Marie Healy, 2012).

Hence, each member state has an obligation to Build Resilience in accordance with Article 3 of the North Atlantic Treaty – the obligation to collectively and individually develop capacities to respond to any form of threat or crisis that aims to threaten society and democratic values and to destabilize the functioning of state institutions.

Resilience and Article 3 – Civil preparedness is a central pillar of Allied resilience and contributes to the achievement of the Alliance's collective defense.

The principle of durability in Article 3 of the founding agreement of the Alliance: "In order to more effectively achieve the goals of this Agreement, the parties, separately and jointly, through continuous and effective self-help and mutual assistance, to maintain and develop their individual and collective capacity to resist armed attacks".

Article 3 helps give NATO the means to fulfill its core tasks, especially the realization of collective defense. The individual commitment of each Ally to maintain and strengthen its resilience reduces the vulnerability of NATO as a whole. Resilience is first and foremost a national responsibility.

NATO agreed on seven basic requirements for national resilience against which allies can measure their level of preparedness; these requirements reflect the essential functions of continuity of government, essential services to the population and civilian support of the military.

In 2016, the Warsaw Summit was held where the allied leaders decided to strengthen NATO's resilience. These seven basic requirements determine the following contents:

These seven basic requirements determine the following contents:

- Continuity of government and critical government services ensured: for example the ability to make decisions, communicate and implement them in crisis conditions;

- Flexible energy supply: back –up plans and electricity networks, internal and cross-border;

- The ability to effectively deal with the uncontrolled movement of people and to deconflict these movements from NATO military deployments;

- Ability to deal with mass casualties: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secured;

- Resilient civil communications systems: ensuring that telecommunications and cyber networks function even in crisis conditions with sufficient backup capacity. This requirement was updated in November 2019 by NATO Defense Ministers, who highlighted the need for reliable communications systems including 5 G, robust options for restoring these systems, priority access to national authorities in times of crisis and through assessments of all risks to communication systems;

- Resilient transport systems: ensuring that NATO forces can move quickly across Alliance territory and that civil services can rely on transport networks, even in crisis situations.

5. INSTRUMENTS FOR DETECTING AND DEALING WITH HYBRID THREATS

The Strategy for Building Resilience and Dealing with Hybrid Threats from 2021, identifies instruments whose application is aimed at creating the ability to detect and reduce vulnerability to hybrid threats (see more about this https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf).

The application of these instruments seeks to increase the ability to respond in accordance with the framework established by NATO and the European Union. The activities of the state are divided into six areas of operational activities – political instruments, economic instruments, military forces, civilian instruments, information instruments and the need to protect critical infrastructure.

Political instruments – A key effect to be achieved in the sphere of politics is the continuity of power. For that purpose, a system for early warning and notification of possible threats will be built, as well as identification and training of key personnel. An effective crisis management system will also be provided to support government activities in times of crisis with spare capacities for independent operation for a period of one month, as well as secure communication links. The following activities are undertaken in this area: achieving protection of the election process from hybrid threats, hostile cyber-activities, information operations conducted by other state and non-state entities and financing of political parties, politicians and non-governmental organizations by external factors.

Economic instruments – The second area of operational activities is the consideration of the economy and favorable business climate. The effect to be achieved in this area is the establishment of a functional mechanism for inclusion of risks related to foreign direct investment. Creating conditions for the development of the domestic economy should additionally achieve significant trade and energy independence. Creating conditions for a digital economy will enable domestic companies to compete in world markets, especially in the European Union market, as well as create new jobs and their rapid transformation of market changes. An essential activity in this area is the fight against corruption.

Military forces **–** The third area of operational activities is: the security-defense sector, that is the military and security forces and institutions. In this area, it is crucial to build the capability of the military security forces and the capacity to manage and support in times of crisis, in order to increase the resilience of society to deal with hybrid threats. The fact that the use of

conventional armed forces is minimized in the case of a hybrid threat indicates the need for continuous improvement of the defense and security mechanisms. In this regard, it is necessary to achieve a high ability to deal with multiple simultaneous attacks on civilian and military targets, the ability to establish an effective mechanism for security of food and water resources, dealing with uncontrolled movement of significant numbers of people and dealing with incidents that have resulted with many casualties. In addition, the intelligence entities of the Republic of North Macedonia should maintain continuous mutual cooperation and cooperation with the intelligence institutions of the EU and NATO, responsible for the assessment of hybrid threats.

Civil instruments **–** The fourth area of operational activity is civil society. In fact, hybrid warfare is designed to achieve social divisions and provoke riots to overthrow the government, primarily through disinformation and psychological operations. Therefore, it is necessary to create the ability for critical awareness and media literacy among the citizens of the Republic of North Macedonia. A high level of inter-ethnic and inter-religious tolerance should also be achieved in the civil sector.

Information instruments – The fifth area of operational activities is the information sector. A key effect needed to deal with hybrid threats in this sector is the creation of the ability to detect misinformation and psychological operations, as well as the ability to deal with Internet "trolls" and use artificial intelligence in the process of spreading false news and misinformation. One of the effects to be achieved is the creation of a permanent and effective system for strategic communication, directly led by the Government of the Republic of North Macedonia and in cooperation with other relevant state institutions. In addition, a situation should be reached in which the public service broadcaster will carry out planned activities to deal with false news and misinformation. At the same time, the state will support the citizens' associations that are active in dealing with misinformation.

The sixth area of operational activities is the protection of critical infrastructure of the Republic of North Macedonia. The first effect to be achieved is the adoption of a legal solution that will determine the critical infrastructure, as well as the adoption of regulations for its protection. In this context, the regulations of the European Union and NATO will be a framework for the future activities of the Republic of North Macedonia in determining and providing critical infrastructure.

Another essential element in dealing with hybrid threats related to critical infrastructure is the diversification of energy sources and suppliers. To achieve this, it is necessary to have infrastructure that will enable a high level of energy independence of the Republic of North Macedonia from individual external energy suppliers. The same concept of avoiding addiction should be used in relation to infrastructure based on new technologies such as mobile, internet and satellite communication. The Republic of North Macedonia, in terms of determining the critical infrastructure and planning its security, will take into account the technological development and the impact of new high technologies.

The Republic of North Macedonia should create a secure traffic infrastructure, reliable energy sources and transport, telecommunications network, stable health and social system, independent media and economic-financial system, as a basic part of critical infrastructure, because the complexity of hybrid threats requires full involvement of all institutional actors in the national security system.

6. CONCLUSION

Building resilience is a long-term process that needs to be context-specific and embedded in national development policies and planning. In order to realize the protection of national interests and create national resilience of society, each country needs to build an effective concept for dealing with a series of challenges as well as defense against cyber and hybrid threats – each country should be able to adapt to the unpredictable, complex and a changing security environment.

In building national resilience, the use of following three methods: detection, rejection and response.

Detection of the threat **–** As a way to deal with hybrid threats, detection implies having the ability to obtain relevant and timely information about the attacker's potential intentions from all domains and media. Due to the complex nature of hybrid threats, stakeholders in all fields need to develop early detection methods (in Macedonia this role is played by the National Coordinating Council of the Intelligence – Security Community). The method to be used to successfully detect threats includes identifying critical national vulnerabilities, associating the vulnerabilities with possible scenarios and assumptions about an attacker's goals and capabilities and determining indicators to link the vulnerabilities and measures to be taken to address the hybrids threats.

Rejection of the threat **-** The ability to repel a threat is a method aimed at building resilience, building the capacity to withstand stress and the ability to overcome the damage caused by threats, as well as the ability to retaliate against an attacker. Resilience is needed, above all. In areas targeted for hybrid attack, such as politics, economics, the defense and security sectors, the information sector, civil society and critical infrastructure.

Response to the threat – Responding to hybrid threats means having an effective decision-making process at the strategic level. In Macedonia, the responsible body for giving directions, making conclusions and proposing measures to respond to hybrid threats, as a threat to national security, is the Council for Coordination of the Intelligence-Security Community (See more about this https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf).

A key factor in this process is having a credible assessment of the situation and determining the level of threat tolerance, the overcoming of which would indicate that the country is subject to attack using hybrid methods. It is therefore necessary to realize effective inter-institutional communication and cooperation, coordination of intelligence services and a fast and efficient political decision-making process. Availability of credible and timely information on hybrid threats against the Republic of North Macedonia will assist the decision-making process, as well as the process of activating the assistance mechanisms of the European Union and NATO's collective defense system. Various mechanisms can be used in response to a hybrid attack, such as economic sanctions against countries, companies and individuals, expulsion of diplomats, intelligence operations and other activities to neutralize hybrid threats. However, it is essential that the response be modeled in a way that does not cause the threat to escalate, but will force the attacker to discontinue hybrid activities due to their ineffectiveness, as the damage they will suffer from such activities will outweigh the potential benefits.

In order for each national country to efficiently and effectively deal with hybrid threats, the author makes the following recommendations: Establishing cooperation with EU and NATO institutions, intended to deal with hybrid threats; the complexity of hybrid threats requires the full involvement of all institutional stakeholders in the national security system; Promotion of cooperation and exchange of information at the national and international level; Building high-

quality and trained key personnel, as well as maintaining the basic principles of national security and resilience of society through constant basic training.

REFERENCES

Zolli A., Healy A. M. (2012). Resilience: Why Things Bounce Back (New York, Simon & Schuster), 7. Italics in original.

Caves B et al. (2021). "Enhancing Defence's Contribution to Societal Resilience in the UK", RAND Corporation.

Hybrid CoE. (2022). Hybrid threats as a concept. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (accessed on 10.06.2023);

Resilience and Article 3. (2021). NATO

Steingartner, W., Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18 (3).

http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf

https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (accessed on 10.06.2023);

https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf accessed on 15.05.2023).