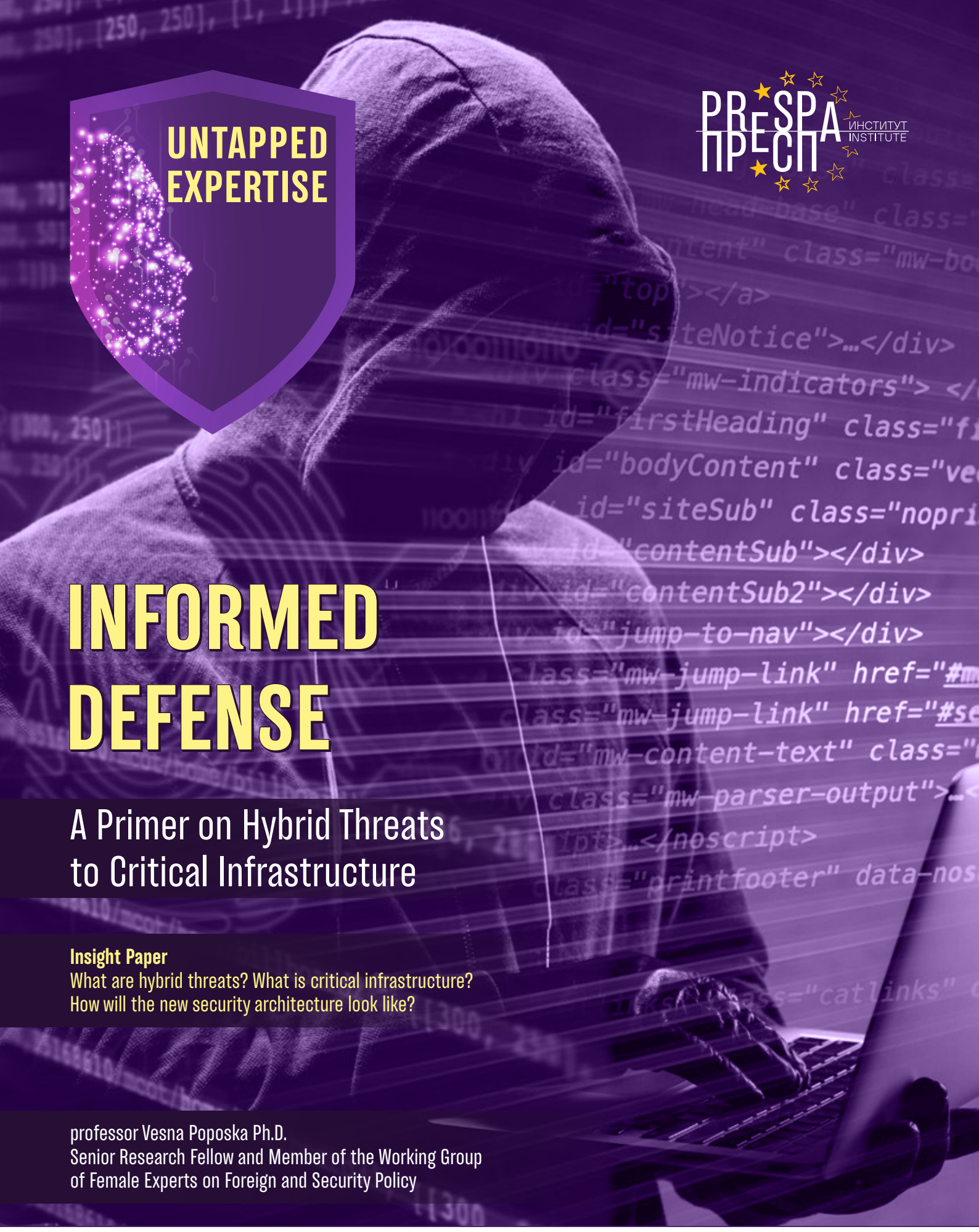

UNTAPPED EXPERTISE

PRESPA ИНСТИТУТ INSTITUTE

INFORMED DEFENSE

A Primer on Hybrid Threats to Critical Infrastructure

Insight Paper
What are hybrid threats? What is critical infrastructure?
How will the new security architecture look like?

professor Vesna Poposka Ph.D.
Senior Research Fellow and Member of the Working Group
of Female Experts on Foreign and Security Policy

Canada

CFLI/FCIL
Canada Fund for Local Initiatives
Fonds canadien d'initiatives locales

INFORMED DEFENSE

A Primer on Hybrid Threats to Critical Infrastructure

Insight Paper

What are hybrid threats? What is critical infrastructure? How will the new security architecture look like?

Published by: PRESPA Institute - Skopje

For the publisher: Andreja Stojkovski, Executive Director

Author: professor Vesna Poposka Ph.D., Senior Research Fellow and Member of the Working Group of Female Experts on Foreign and Security Policy

Design and layout: Brigada Design ltd.

Skopje, January 2024

This publication is part of the Untapped Expertise project supported by the Embassy of Canada through the Canada Fund for Local Initiatives. The views, findings and conclusions or recommendations arising from the publication or the project are the responsibility of the authors and the supported partner organization, and do not necessarily reflect the views of the funding partner and its respective government.

Insight Paper
What are hybrid threats? What is critical infrastructure?
How will the new security architecture look like?

CONTENT

I. INTRODUCTION

1.1. WHAT ARE HYBRID THREATS?

Hybrid threats[1] – unconventional threats that fall below the threshold of military force – have become a ubiquitous feature of today's security environment.

The rise of hybrid threats represents an extremely subversive threat to national security and the international order. Due to the diversified and subtle forms of action, there is no consensus on their definition. In essence, the term hybrid threat refers to different type of activities that are strategically planned and coordinated under the cover of states, that is, other entities, as a tactic to exert influence in order to change or cause damage to the existing order.

In this case, a "**victim**" can be any individual or institution with decision-making power at the local, regional, state or institutional level. Such actions are deliberately aimed at any sphere that is potentially vulnerable, or represents a potential field for the abuse of civil rights and freedoms. Although they exist in every context and probably no state is immune to them, the most susceptible to their effects are new democracies or states in transition and building democratic institutions. That is why, unfortunately, they are a tool through which certain spheres of influence are built. However, a large part of what is treated as a "**hybrid threat**" is not a novelty at all - but a strategy and tactic applied in a new way, because "*war has a changing nature, but a permanent character*".[2] Hybrid threats in any given context take on a new form and dimension, especially due to increased digitalization and dependence on Internet services.

Under hybrid threats, in the narrowest sense of the word, is meant a different set of non-military activities through which strategic goals are achieved. They are a counterweight to conventional threats, that is, to the threat of using military force. Most often, the bearers of hybrid threats are states, but sometimes they also come from other entities, such as terrorist groups, criminal organizations, even hacktivists.[3] In a broader context, the term hybrid threat refers to multimodal, low-intensity, kinetic, but also non-kinetic threat that includes multiple tactics: cyber-war, asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, etc.

Recognized in NATO's 2010 Bi-Strategic Command Concept[4], hybrid threats are defined as "*those posed by adversaries with the ability to simultaneously use adaptive conventional and unconventional means in pursuit of their objectives.*" The term "**hybrid threats**" is used as an "umbrella" that covers a wide range of emergent forms of security threats that can come from states, but also from other entities, and there is a difficulty in proving attribution and responsibility.

In the joint communication[5] of the European Commission, the European Parliament and the Council on the European Agenda for Security and Common Defence from 2016, the concept of hybrid threats is defined as a mixture of coercive and subversive activity, using conventional and unconventional methods (i.e., diplomatic, military, economic and technological), coordinated by states or other entities to achieve specific goals while remaining below the threshold of formally declared war.

In practice, hybrid threats are a variety of influence operations through which, under the guise of democracy and liberal space, various malignant actors (mostly, but not exclusively foreign) achieve a strategic goal in their favour. They are always aimed at achieving strategic goals, and are synchronized, that is, in this case, trouble never comes alone, because it is about synchronized actions that may have a specific goal, such as, for example, a change of government, or a general goal for creating panic among the population and mistrust in the institutions. At different stages of implementation, hybrid threats can take different forms (violent protests, cyber-attacks, false reports of planted bombs, fake news) and be carried out by different entities, including political parties, non-governmental or religious organizations. Hybrid threats are aimed at creating public opinion that would help achieve the desired effects for the client or the centre of power from which they are directed, and their effects are cascading, that is, they are not always obvious. Therefore, it is extremely important to build personal and social resilience, as well as a society of conscious, informed, and free individuals and media.

1 https://www.iss.europa.eu/content/protecting-europe-0

2 Carl von Clausewitz (https://en.wikipedia.org/wiki/Carl_von_Clausewitz)

3 Eng. *Hacktivist – a person who makes unauthorized access to computer files or networks in order to achieve some social or political goals.*

4 https://www.nato.int/cps/en/natohq/topics_82705.htm _ _

5 https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF

1.2. WHAT IS CRITICAL INFRASTRUCTURE?

In the new security environment, hybrid threats are mostly aimed at critical infrastructure, which as a security and operational term is a relatively new phenomenon and became especially relevant after the Russian attack on Ukraine, covering mostly energy and transport systems, but also water supply systems, as well as traffic infrastructure. Although the term is new, it does not mean that critical infrastructure did not exist before. On the contrary, every social order in every age of human development had its own critical infrastructure, that is, systems essential for social functioning - water supply, food production and supply, certain road corridors. In the changed security environment, critical infrastructure is a legitimate object of protection that must be recognized by the system as such through the imperative of the norm, that is, the legal framework. To be able to protect the critical infrastructure, but also to protect ourselves, first, it must be recognized by the national legislation. In the Republic of North Macedonia, this will happen with the adoption of the first Law on Critical Infrastructure, which is in the final stages of adoption.[6] At the same time, it is important to emphasize that defining the national critical infrastructure is not a deterministic and final process, but a dynamic and proactive one. Critical infrastructure and its definition may be subject to change in accordance with the risk assessments of each national government.

The European Union defines critical infrastructure through the directive on the determination and identification of European critical infrastructure from 2008[7], which calls on the member states to identify and determine the critical infrastructure they have on their territory, as well as to carry out an assessment of the need to improve her protection. All Member States have implemented the Directive by establishing a process for identifying and designating European critical infrastructure in the energy and transport sectors. In the Directive itself, critical infrastructure is defined as: "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*" The Directive specifically recognizes European Critical Infrastructure (ECI) as critical infrastructure whose disruption or destruction would have a cross-border effect and which should, as such, be singled out and identified through a common procedure. Towards the end of 2022, the European Commission [8] went a step further by defining critical entities as a more complex form of critical infrastructure with increased interdependencies.

In the Tallinn Manual [9], critical infrastructure means physical or virtual assets and assets under the jurisdiction of the state, which are so vital that their disabling or destruction could weaken national security, the economy, public health and safety, or the environment.

"Protection of critical infrastructure" generally means a set of measures and activities of a different nature aimed at maintaining, improving, and preserving the character and functionality of critical infrastructure as such. In that context, different sectors or different countries understand the protection of critical infrastructure differently.

The danger of the critical infrastructure from hybrid threats is mostly due to the fact that, in general, the critical infrastructure represents the so-called "soft target". The term "soft targets"[10] is usually associated with places where people gather in large numbers, such as museums, cinemas, religious sites, shopping malls, etc. Soft targets are contrasted with so-called "hard targets", which are widely identified places where high levels of protection are provided, often by armed personnel, i.e., locations where public access is restricted or subject to heavy controls (for example, military installations). Finally, critical infrastructure may be a soft target, but, all soft targets are not critical infrastructure. The key element of distinction relates to the issue of "criticality". Soft targets do not necessarily appear to be critical to the provision of basic social services. Such are, for example, stadiums and concert halls.

6 https://mod.gov.mk/javna-rasprava-zakon-za-kriticna-infrastructura/

7 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF

8 https://eur-lex.europa.eu/eli/dir/2022/2557/oj#:~:text=Council%20Directive%202008%2F114%2EC%20%284%29%20provides%20for%20a%20procedure ,cross-border%20impact%20on%20at%20least%20two%20Member%20States .

9 https://ccdcoe.org/research/tallinn-manual/

10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0200

1.3. LEGAL FRAME

There is no single legal framework for responding to hybrid threats, just as there is no single definition. That is why the answer will depend on the context and a case-by-case analysis will always have to be done in order to give an appropriate answer and set an appropriate framework for action. In doing so, it should be taken into account that international law has four vital functions: 1) *to define precisely the limited cases in which the use of force is permitted* (self-defence and preservation or restoration of world peace and security, in accordance with the Charter); 2) *to regulate and control the use of force* (even) *in situations where it is allowed*; 3) *to evaluate whether the force that was used was illegal*; and 4) *to regulate the consequences of the use of force*, whether it is permitted or not. Given the four vital functions and the fact that international law regulates the use of force through the prohibition of use and exceptions to that prohibition, efforts to maintain world peace and security have created four aspects to regulate the use of force in international law. The same sources of law apply to all four aspects, in accordance with Article 38 of the Statute of the International Court of Justice: 1) international agreements; 2) international customary law; 3) the practice of the states; 4) the opinions of prominent jurists; and 5) judicial practice.

The first aspect of the four mentioned is *ius contra bellum,* that is, the right against war or against the use of military force. The second aspect is the corpus of legal rules *ius ad bellum,* that is, the law of war, which regulates when it is legally permissible for a state or states to resort to the use of force. The third aspect is the corpus of legal rules *ius in bello* which governs the principles, standards and regulation that come into force when force has already been used and there is an active conflict. The fourth aspect is *ius post bellum,* or principles, standards, and obligations after the end of major hostilities. Hence, the normative framework on the basis of which to operationalize the protection of critical infrastructure, or on the basis of which to respond to hybrid threats, may differ from case to case. Sometimes national law is applicable, sometimes international conventions, and in a third case, it can be for parallel processes. This is particularly evident in dealing with terrorism and organized crime.

The two most serious challenges in dealing with hybrid threats are the difficulties to establish a causal and jurisdictional relationship, that is, to prove responsibility and prosecute criminal prosecution in an international, and especially cyber, context.

II. WHERE DO HYBRID THREATS COME FROM?

"Doctrine of Gerasimov"[11] is a concept that refers to hybrid threats primarily as operations to achieve influence through informational, cultural, humanitarian, diplomatic and economic activities. These include fake news that influence the creation of public opinion, so in that context, the false bomb alerts, which we have lived with for a certain period of time since 2023, aim to instil fear and mistrust in institutions. Although the "Gerasimov Doctrine" is more commonly used as a Western coinage, the term derives from a text by Russian Army General Valery Gerasimov, published precisely in the period when Russian-Ukrainian relations were quite strained ten years ago, followed by the annexation in the Crimea.

Of course, it is unfair to attribute the entire burden of hybrid warfare to General Gerasimov alone. This doctrine has its historical development both in Russian foreign policy and in the development of intelligence services. It is considered by many to be an upgraded version of the "Primakov Doctrine" named after the former Minister of Foreign Affairs and Prime Minister of the Russian Federation, Yevgeny Primakov, who states that a monopolar world dominated by the United States is unacceptable for Russia and offers the following principles for Russian foreign policy.[12]

- Russia to strive for a multipolar world that can counterbalance the unilateral power of the United States.
- Russia to insist on its primacy in the post-Soviet space and to lead the integration in that region.
- Russia to oppose NATO expansion.

In the following years, the impression was created that the threat from Russia is exclusively based on soft power, which is realized only through hybrid threats. However, the war with Ukraine showed that, unfortunately, this was not the only danger coming from the east. The scale and scope of Russian hybrid warfare operations have expanded with the growth and improvement of Russian capabilities for so-called "hard power", that is, the armament and use of force.

Russia has a long history of propaganda and disinformation operations classified according to their effects: information-technical and information-psychological.[13] A major turning point for these efforts occurred in 2008 when pro-Russian cyber-attacks coincided with Russian military operations in Georgia. Both sides competed to control the flow of information to the international community. From today's perspective, the expert public is pretty much in agreement that Georgia won the information war[14] through its own aggressive campaign using disinformation and media manipulation, which is a rather dangerous precedent for the idea of democracy, freedom, and liberal values. While the Russian part of the story is certain, it is far from the only source of power from which hybrid threats come. Battles for strategic supremacy and geopolitical dominance, in different regions of the world, involve different actors.

11 https://www.heritage.org/defense/report/understanding-russias-concept-total-war-europe
12 https://carnegieendowment.org/files/Rumer_PrimakovDoctrine_final.pdf
13 https://www.marshallcenter.org/sites/default/files/files/2020-03/percon_v10n1_eng_0.pdf
14 https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

III. POSTULATES OF THE NEW SECURITY ARCHITECTURE

The contours of global change can be defined on several fronts. **First**, there is the change of actors, which is due to a redefinition of power relations between existing actors - states, and the emergence of new actors - transnational corporations, non-governmental organizations, terrorists, global rebels, organized criminal networks, mafia cartels and other atypical structures. With the inclusion of regular state elites in the concept of democratization, the opposition took the form of "private", entities that use terrorist methods filling in the space of the global order.

Second, international law does not recognize new actors as subjects. The regimes were only later recognized as a new threat to world peace and security. The way in which the response to such situations was or was not organized greatly redefined the map of global hotspots.

Third, the increased awareness and rapid flow of information has made public reactions inevitable, especially through the popularization of social media. The influence of public opinion has increased and the flow of information influencing its creation at a distance of thousands of kilometres is incredibly fast.

Fourth, the increasing degree of radicalization, in every sense, leads to increasing divergence of interests of individuals and groups, at the expense of the ideal of open societies. Radicalization is in part a response to the narrowing of the liberal space, but in a much larger part, a response to economic and social inequality, the loss of meaning, the search for identity, increased fear and setting boundaries between diversity, irresponsible leadership and populism. European pan-idealism under the impact of the economic and migrant crisis was largely replaced by Orbanism and culminated in the Brexit vote. The radical right, neo-fascists and related groups entered the national parliaments of countries that promoted democracy as a concept. The only quick response was social movements and protests around the world, which, in turn, were much more misused for other interests.

Fifth, increased industrialization and uneven industrial development have led to an environmental disaster and intensified the effects of global warming.

Sixth, technological advances have enabled the accumulation of power in the hands of individuals with malicious intent. The (mis)use of cyberspace and the benefits of modern technology enable large reach and quick gain to achieve various political goals.

Seventh, transnational companies whose capital is larger than the budget of many countries, in the race for profit and the fight against competition, involve them in networks that traditionally did not affect the business sector. Democracy and capitalism that spread from west to east inhibited processes of rapid transition and privatization. The transformation of capital from social to private overnight led to typical sectors of critical infrastructure passing into the hands of private businessmen from abroad or directly owned by the old elites, thus both multiplying their own power and opportunities to exercise influence on making decisions of national interest. Privatization of services led to redefining the roles that certain institutions had, especially in the security sector, and some of them to be handed over to private entities, which operated in the middle space for a long time due to the lack of precisely defined powers of both the other side.

Eighth, because of everything stated above, the concept of war has changed drastically. Power is redefined, and the balance of power is out of balance.

In summary, the conclusion is that the security environment has changed drastically. New relationships and new threats require different approaches and new responses. The crisis of values negatively affects the balance between the imperative for freedom and the need for security, narrowing the liberal space of the contemporary conceived societies.

IV. REDEFINING THE TOOLS OF NATIONAL POWER

The new security environment and new actors challenged the status quo and the power of nation-states, whereby the instruments of national power were gradually redefined. The emergence of a new strategic environment requires the orchestration of multiple instruments of power[15]. This process started with the concept of **DIME** (*Diplomacy, Information, Military, Economy)* which was gradually upgraded, to finally be supplemented with **FIL** (*Finance, Intelligence, Law-Enforcement* - **DIMEFIL)**. In such a constellation of relationships, recognizing and dealing with hybrid threats is even more difficult. The border between war and peace is constantly shifting and expanding. Rival states are increasingly using hybrid tactics to influence democratic processes and exploit the vulnerabilities of their adversaries. These tactics[16] involve the coordinated and synchronized use of violent and nonviolent instruments of power to carry out cross-domain actions from the threshold of conventional armed military conflict, often bypassing detection, and attribution.

15 https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106566/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

16 https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf

V. PRACTICAL EXAMPLES

5.1. CYBER OCCUPATION

In 2007, the Estonian government announced that it would move a monument called the Bronze Soldier[17] from the centre of Tallinn to a military cemetery on the outskirts of the city. The monument was erected by the Soviet authorities in memory of the Soviet forces that defeated the Nazi army from Estonia. Many Estonians found the monument offensive due to the decades-long occupation of the country by the Soviet Union. The decision at the time caused outrage in the Russian-language media and led to two days of rioting in Tallinn in which 156 people were injured and 1,000 people were detained.

A day later, Estonia was hit by cyber-attacks, which lasted several weeks and affected Estonian banks, government bodies and the media. The cyber-attacks[18] came from Russian IP addresses, although the government has always denied any involvement. *Russian hacking group* **Kilnet** claimed responsibility for the attack[19], saying on its Telegram account that it had blocked access to more than 200 state and private Estonian institutions, including the online citizen identification system. The series of activities that followed turned Estonia into a leader in cyber resilience, and NATO established a cyber excellence centre in Tallinn.

5.2. ELECTION INTERFERENCE AND DISINFORMATION

In an era when disinformation has become a political strategy, it is extremely difficult to discern the truth, both for voters and journalists. In recent years, several spectacular attempts at election interference have occupied the news. From the Russian Intelligence Research Agency (IRA) interference in the 2016 US election[20] to the hacking and leaking operation targeting French President Emmanuel Macron. One thing is, however, common to all. Their design, as well as the timing of electoral interference, showed determination to completely disrupt the electoral process.

In an electoral context, disinformation, through fake news or manipulations, is of great importance, because it affects the creation of public opinion and thus the behaviour of voters. Manipulations can consist of false behaviours, used to reinforce a political message through ***bots*** or ***trolls*** on social networks, that is, by inciting real-life events, especially demonstrations. Disinformation, as false content, can be used as targeted lies that promote one candidate or denigrate another, that is, simply undermine trust in the correctness of the electoral process. That is why the Secretary of National Security of the United States, in 2017, added the electoral system of the United States[21] to the list of critical infrastructure as the seventeenth sector. Considering the sovereignty of the federal states in relation to elections, such a decision was not met with enthusiasm.

5.3. EMAIL HOAX

The government of Lithuania was the target of an email hoax claiming that NATO troops were withdrawing from its territory.

NATO Secretary General[22]Jens Stoltenberg said that a fake letter sent on his behalf announcing the alleged withdrawal of allied troops from Lithuania was intended to confuse citizens and undermine the unity of the allies, using the pandemic. The dominant narrative of the related fake news was about how NATO was threatening the interests of allies, allied soldiers were behaving inappropriately in public, and the alliance was working to build nuclear weapons instead of helping to deal with the pandemic.

17 https://www.slobodnaevropa.mk/a/31990820.html
18 https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web- wa
19 https://www.slobodnaevropa.mk/a/31994141.html
20 https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/
21 https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf
22 https://www.dw.com/en/malign-actor-poses-as-nato-chief-emails-lithuania-saying-troops-are-pulling-out/a-53209653

5.4. Religious Affairs

Montenegro faced political turmoil shortly before joining NATO. There was turmoil after that as well. They were the result of various apparently social issues, and the most pronounced were those connected with religious issues.[23] The demoralization phase included an overwhelming presence of fake news, hate speech, disinformation, and calls for defence against an imagined enemy. In the campaign to spread fake news and misinformation, one portal[24] played a leading role by creating a serious amount of misinformation. Although the portal was not registered in the Media Registry, it presented itself as a journalist. In doing so, he created a lot of content aimed at provoking an emotional reaction from readers, using the abuse of historical contexts, and connecting the President of Montenegro with the fascist regimes of the Second World War. Pro-Kremlin Sputnik acted similarly. The cases of disinformation by these two portals were documented by the digital forensic centre in Podgorica.

5.5. Asian hegemony

On October 12, 2020, India[25] faced its worst power outages in decades. With the economy crippled, the stock market closed, thousands of travellers stranded, and hospitals scrambling to provide back-up options for their COVID patients. Major power outages are not entirely uncommon in India, but they came as a surprise to the capital of the western state of Maharashtra, Mumbai. The authorities in Mumbai were stunned and went in search of an answer. The investigation showed that the cause of the interruption in the supply of electricity was a cyber-attack that targeted the servers of the state electricity companies. Although they failed to prove responsibility, for the authorities the implication of Chinese hackers was more than clear. In its bid to establish Asian hegemony, China sees India as a major obstacle. This possible sabotage came at a time of heightened military tensions, with confrontations flaring up at numerous points along the disputed border between the two countries. Beijing's ability to pressure its neighbour extends beyond the conventional battlefield and increasingly includes unconventional forms of warfare.

5.6. Thawing the frozen

The escalation of the Israeli-Palestinian conflict, as well as the conflict in Nagorno-Karabakh, as the situation in Ukraine developed, were not an absolute coincidence, but an attempt to dilute the concentration of international aid and the focus of public opinion from Ukraine to different points in the world. Hybrid threats may take different forms in different regions, but they have the same source and a similar goal, which does not go beyond what is considered a sphere of national interest by very few centres of power. So far, we have seen proxy activities through media and disinformation, cyberspace, humanitarian affairs, religious issues, bilateral disputes, energy security, critical infrastructure disruption and general division that creates a biased atmosphere. Social and political polarization will not reduce the pressure in the time to come.

[23] https://nsf-journal.hr/online-issues/focus/id/1296
[24] https://www.in4s.net/
[25] https://www.foreignaffairs.com/articles/china/2021-04-02/chinas-unrestricted-war-india

VI. RESISTANCE AS A COMMON RESPONSE

To help counter hybrid threats and support policy makers in the defence of democratic societies, Hybrid CE and the European Commission's Joint Research Canter[26] have built a model that recommends a framework for a comprehensive resilience review. The **Comprehensive Resilience Ecosystem (CORE**) highlights two factors when considering a response. *First,* open societies are always more connected internally and with each other. *Second,* any response should involve the whole of society to effectively counter the threats. For this purpose, the presented model refers to different social or sectoral "spaces" (institutions, civil society, services), as well as different "levels" (international, national, and local).

The concept of resilience[27] is the latest security concept in crisis management and civil protection in the EU and NATO. At the same time, the degree of resilience (elasticity, i.e., the ability to return the vital functions of society to normal very quickly after facing a crisis) determines how quickly a society can respond to the crisis and restore the vital social functions to function after the occurrence of a crisis situation.

By building resilience, a unique response can be given to threats of a different nature, regardless of the emerging form. It implies a holistic approach, strategic communication, centralized management and decentralized execution, based on the human rights approach. Clear legal and operational frameworks that are compatible with the protection of human rights should be established, as well as emphasizing that crisis management is important not only in the case of terrorist attacks, but also in small incidents to avoid or reduce the impact and escalation of the crisis. The identification of an appropriate crisis management framework requires consideration of two fundamental issues. *The first* is whether emergency management will follow a specific risk or hazard approach, or will have an *all-hazards approach.* Both approaches have advantages and disadvantages. When crisis management structures are in place for certain types of threats, dedicated processes can be put in place. However, choosing a hazard-specific approach can be problematic when the nature of the incident is not clear, as it can cause uncertainty about the applicable intervention framework. *The second* question should address whether the extent of crisis management structures and procedures should be sector-specific or cross-sectoral. If the first approach is chosen, the legal framework is often adopted by the ministry responsible for the specific sector or the sector regulator. Instead, a cross-sectoral approach is often regulated by general legislation.

A recommendation for overcoming the situation is the application of the *all-hazards approach,* that is, the approach of addressing all hazards. It is especially important to see the big picture, that is, to place critical infrastructure in a broader rather than isolated context - for example, although international environmental law does not directly address critical infrastructure, it can nevertheless affect certain segments. These aspects are important because prevention is a key link in building resilience.

An effective strategy for the protection of critical infrastructure mainly rests on two pillars: an effective **early warning system** and effective **crisis management.** The successful functioning of these two systems contributes to risk reduction measures, which, in turn, increases the security of critical infrastructure. An effective strategy for the protection of critical infrastructure in that context should provide an effective risk assessment and an appropriate framework for action. The danger from other entities that have a networked and global setting, but also from potential natural disasters, in conditions of a large number of entities (from the public and private sector, with different interests, and at the same time interdependent in the domain of providing services), imposes the need for centralized way of decision making. The centralized way of making decisions, no matter how old-fashioned and liberal it may seem at first glance, is necessary for two reasons: *First,* it ensures effective coordination in the field of early warning. All involved actors receive necessary information about the situation with the potential danger of natural disasters. *Second,* with the centralized way of making decisions, all actors apply the same set of measures and standards.

Threats will continue to grow and mutate. However, effective protection lies in prevention and strengthening society - and in strengthening the legal framework in that very segment. It implies legal amendments and the application of best practices, with the establishment of the entire institutional framework resulting from it, as well as the effect of the fiscal implications. However, even the best legal solution will not be effective without an implementation mechanism and without predicting appropriate fiscal implications for it. Ultimately, building partnerships is necessary, but they should be based on a strategic and institutional approach, encompassing the academic and business community, government institutions and civil society, with a vision of building a resilient society based on education and cyber culture.

[26] https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

[27] https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity .

VII. NORTH MACEDONIA - CHALLENGES AND RECOMMENDATIONS

North Macedonia's membership in NATO contributed to the national system relatively quickly taking over certain processes and concepts. Thus, in the area of policy making, a whole series of strategic documents of exceptional importance were adopted, such as **the Strategy for Cyber Defense**[28]and the **Strategy for Building Resilience and Dealing with Hybrid Threats**[29]. At the same time, the Strategy for Building Resilience is set quite broadly, although there are no annual progress reports, in particular since some of these issues run through the European Commission Country Report on North Macedonia.[30]

According to the Criminal Code, spreading misinformation does not constitute a crime, and Internet media are not regulated by a special law, but are left to self-regulation. This principle is encouraged by international media reporting standards, although in the new context it is insufficient. On the other hand, if you try to prevent disinformation by making it a crime, then you are entering another sensitive area, where it is extremely difficult to strike a balance between the need for security and protection against disinformation and what constitutes a standard of freedom of speech, in accordance with Article 10 of the European Convention on Human Rights. The liberal perimeter is increasingly narrowed precisely because of the new type of threats in a new security environment, and personal liberties are put on the back burner in the name of the fear of the pandemic, the hybrid war, inflation, the real war in Ukraine, the millions of refugees from the Middle East.

Canada can be an example of such a policy[31], which, led by a conservative government, adopted new anti-terrorism legislation in 2015, and in 2017, led by a liberal government, established new powers for the national electronic surveillance agency, giving it the opportunity to work closely with military and conduct offensive actions against foreign entities and shut down potential cyber-attacks in order to protect Canada and its critical infrastructure. This situation meant the legalization of not only anticipatory, but also pre-emptive self-defence in a cyber context, which can be an extremely dangerous practice - that is, to use military force against an attack that has not yet occurred.

That is why, due to the complexity of the problem, it is necessary to build personal, institutional and social, that is, national resilience, as well as awareness of the dangers. Although resilience is an extremely broad concept, it is undeniably necessary to start from the basic postulates of the most pronounced problems that the new security environment would potentially cause. A new national security assessment is necessary, as well as a new risk assessment methodology. Additional regulation in the media sector is necessary, as self-regulation is obviously not enough. That regulation should certainly not go in the direction of narrowing the freedom of the media, but in their protection and promotion, that is, the imposition of equal conditions and responsibility for electronic portals, but also for other registered media. This additional regulation should not affect the establishment of the media, but should create a register of real owners and guarantee the designation of an imprint with editorial responsibility. With that, traditional media, journalists and editors who professionally perform their task, will not be put in a disadvantageous position. Also, the sources of funding for the media as well as the change in the funding model are issues that need to be further considered. The same applies to the financing of political parties and campaigns. A matter of particular concern is the rise of the radical right and its open support for undemocratic systems. Hence, media literacy and fact-checking services are of particular importance, as well as active institutional transparency. While, the information landscape[32] plays a role in the assessments of the levels of vulnerability in the Western Balkans. The availability of legitimate information is at the heart of building resilience against hostile influence.

Cyber awareness and cyber culture are also prerequisites for building healthy societies. It implies not only compliance with international standards, but also diversification of power sources and its concentration, as well as reduction of dependencies between different subjects of critical infrastructure, especially in the online world. A systemic approach in this segment would mean changing a series of regulations that at first glance have no direct connection with building cyber capacities, such as, for example, public procurement. Strengthening the institutions' capacities in the direction of digitalization of services and dealing with threats from cyberspace is a necessity. This especially applies to the institutions that have competence in the area of personal data protection and internet security, as well as the development of the national *CERT unit* (Computer *Emergency Response Team* - **CERT)** following the example of Slovenia. Strengthening the media sector and reforming the public broadcasting service are a necessity, as well as protecting the dignity and attractiveness of the journalistic profession. On the other hand, regulation of influencer behaviour and artificial intelligence is needed, probably on a global scale, but a local response is needed.

28 https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf

29 https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf

30 https://neighbourhood-enlargement.ec.europa.eu/north-macedonia-report-2023_en

31 https://www.cbc.ca/news/politics/trudeau-tracker-anti-terrorism-bill-1.3586337

32 https://www.researchgate.net/publication/361700596_Hybrid_Warfare_in_the_Western_Balkans_How_Structural_Vulnerability_Attracts_Maligned_Powers_and_Hostile_Influence

The adoption of the proposal for the Law on Critical Infrastructure, which is in the final stage in the Ministry of Defence, will significantly contribute to the strengthening of resilience. From systemic solutions, a quick implementation of the idea of reforming the system for crisis management and civil protection is necessary, because resilience implies a quick return to normal functioning after a possible shock or crisis scenario, not the absence of crises. In addition, it is necessary to pay more attention to religious organizations and their systemic integration into the wider social constellation. Unfortunately, the anti-gender movements are increasingly gaining momentum, as well as the pro-Russian narrative, precisely by individuals who come from certain ideological prominences. Resilience in dealing with pressure and malignant influences must also be shown by cultural institutions. Especially for those coming from prepared entities, adept at exploiting and manipulating religious and social issues for political gain with disinformation spread through social media platforms, religious and cultural institutions, proxies, and cyber intrusions against networks. In addition, building trust in institutions is still essential for the stability of the system and the government.

To reduce the risks[33] associated with malignant influence, the state must be functional and strong. From there, the fight against corruption, the improvement of public services, the increase of the standard of living, are not only phrases from political speeches in the process of accession to the European Union, but also a need for actively building resilience.

Civil society plays a particular role in the process of building resilience. Civic organizations should continue as an active corrector and observer of the situation, while smaller local organizations, which know the situation in the interior best, should retain the role of creators of social engagement for young people outside the metropolis. Strengthened youth participation in decision-making and policy-making processes is also a defence against negative influences and hybrid threats, and inclusion is the first step towards neutralizing radicals and, as such, is necessary for building strong social communities.

In modern conditions of climate change, but also of Russia's military aggression in Ukraine, building energy independence is an important tool for creating resilience and dealing with the consequences of climate change. No less important is the provision of primary health care resources in regional and local health centres, in order to reduce the burden on central facilities and properly allocate and use resources. Finally, the adaptation of institutions to changes contributes to the acceptance of social dynamics towards hybrid threats, which, although they do not change their essence, change their form and shape daily.

Hybrid threats have a common denominator, but are extremely diversified. That is why, in all critical areas, it is necessary to work on raising awareness and knowledge about critical infrastructure, actively building partnerships and alliances, strengthening the legal and institutional framework, as well as capacity building. A teleological approach and joint response of all involved actors is necessary, as well as promotion of science and education in order to overcome the challenges.

[33] https://intapi.sciendo.com/pdf/10.2478/seeur-2022-0018

BIBLIOGRAPHY

1. Bertolini, Minicozzi and Sweijs (2023) Ten Guidelines for Dealing with Hybrid Threats - A Policy Response Framework, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf

2. CBC (2016) Trudeau tracker: Promised changes to anti-terrorism law C-51 still months away, https://www.cbc.ca/news/politics/trudeau-tracker-anti-terrorism-bill-1.3586337

3. CCDCOE, the Tallinn manual https://ccdcoe.org/research/tallinn-manual/

4. Disinfo.eu (2023) Foreign elections interference - an overview https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/

5. Dolan (2022) Hybrid Warfare in the Western Balkans: How Structural Vulnerability Attracts Maligned Powers and Hostile Influence, https://intapi.sciendo.com/pdf/10.2478/seeur-2022-0018

6. DW (2020) Fake 'NATO' email informs Lithuania of troop pullout https://www.dw.com/en/malign-actor-poses-as-nato-chief-emails-lithuania-saying-troops-are-pulling-out/a-53209653

7. EU (2008) Council Directive 2008/114/EC https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF

8. EU (2017) Communication from the Commission to the European Parliament and the Council on a more Effective Return Policy in the European Union - A Renewed Action Plan , Com/2017/0200 Final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0200

9. EU (2022) Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) https://eur-lex.europa.eu/eli/dir/2022/2557/oj#:~:text=Council%20Directive%202008%2F114%2FEC%20%284%29%20provides%20for%20a%20procedure ,cross-border%20impact%20on%20at%20least%20two%20Member%20States .

10. Euronews (2022) Cyberattacks likely to rise in wake of Ukraine War. This is what Estonia learned from Web War One https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web- wa

11. European Commission (2016) Communication https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF

12. European Commission (2023) North Macedonia progress report https://neighbourhood-enlargement.ec.europa.eu/north-macedonia-report-2023_en

13. Fiott & Parkes (2019) PROTECTING EUROPE - the EU's response to hybrid threats https://www.iss.europa.eu/content/protecting-europe-0

14. Foreign Affairs (2021) China's Unrestricted War on India- Beijing Bullies Its Neighbor by Unconventional Means https://www.foreignaffairs.com/articles/china/2021-04-02/chinas-unrestricted-war-india

15. HybridCoE (2023) Hybrid threats: A comprehensive resilience ecosystem https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

16. Iasiello (2017) Russia's Improved Information Operations: From Georgia to Crimea https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

17. Murphy (2016) Understanding Russia's Concept for Total War in Europe, https://www.heritage.org/defense/report/understanding-russias-concept-total-war-europe

18. NATO (2010) Strategic concept https://www.nato.int/cps/en/natohq/topics_82705.htm

19. NATO (2023) Resilience, civil preparedness and Article 3
https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity .

20. Per Corcordiam (2020)
https://www.marshallcenter.org/sites/default/files/files/2020-03/percon_v10n1_eng_0.pdf

21. Rodriguez, Walton, and Chu (2020) Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106566/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

22. Rumer (2019) The Primakov (Not Gerasimov) Doctrine in Action
https://carnegieendowment.org/files/Rumer_PrimakovDoctrine_final.pdf

23. Trifunovic & Obradovic (2020) Hybrid and Cyber Warfare – International Problems and Joint Solutions
https://nsf-journal.hr/online-issues/focus/id/1296

24. US Elections Assistance Commission (2017)
https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

25. Government of the Republic of North Macedonia (2021) The strategy for building resilience and dealing with hybrid threats.

26. Ministry of Defense of the Republic of North Macedonia (2020) Cyber Defense Strategy

27. RFE/RL (2022) Estonia repels massive cyber attack after removal of Soviet monument
https://www.slobodnaevropa.mk/a/31994141.html

28. RFE/RL (2022) Estonia removes Soviet WWII monuments
https://www.slobodnaevropa.mk/a/31990820.html