Original scientific article
UDK 327:911.3]:351.78(497.7)
UDK 351.86:355.45(497.7)

CRITICAL INFRASTRUCTURE IN THE CHANGING GEOPOLITICAL AND SECURITY LANDSCAPE: A CASE STUDY OF THE REPUBLIC OF NORTH MACEDONIA

Ivona LADJEVAC[1]
Toni MILESKI[2]

Abstract: *The paper aims to analyse the preconditions for constructing a comprehensive critical infrastructure protection system in North Macedonia. Also, in the Republic of North Macedonia, in the last five years, significant progress has been made in moving the national engagement and approach to implement the critical infrastructure protection concept. The Republic of North Macedonia, perhaps the last in the Western Balkans region, has an urgent need for normative regulation of all aspects of the critical infrastructure sphere. The dynamic processes on the international stage rightly give signals in the direction of the essential need for critical infrastructure protection. Changing geopolitical and security landscapes, war, natural disasters, hybrid threats, health crises, energy crises, climate change, and many other adverse processes allude to the conclusion that the disruption of critical infrastructure is increasingly not a matter of escalation but a matter of time.*

Keywords: *Critical infrastructure, North Macedonia, Geopolitics, Protection, Hybrid war, Hybrid threats, Climate change.*

Introduction

There is a growing trend of building resilient societies and resilient critical infrastructure (systems) in NATO and the EU. The European Commission on 16 December 2020 proposed a revision of the existing directives from 2008. These preconditions and processes should be considered when building a Macedonian system to protect critical infrastructure. (European Commission, 2020). In this case, we refer to the review and analysis of relevant literature that shows resilience has no single definition, especially when viewed as an attribute-specific system. A previous study offered a number and different definitions of this concept. At the same time, many studies may find differences in the definition of resilience, as in the case of infrastructure systems.

In particular, when it comes to protecting critical infrastructure, it should be clear that optimal levels cannot be achieved for at least two reasons. The first is the financial nature, while other

[1] Research Fellow and Deputy Director at the Institute of International Politics and Economics – Belgrade, Serbia.

[2] Full Professor at Ss. Cyril and Methodius University – Faculty of Philosophy (Institute of Security, Defence and Peace).

things are constantly evolving and transforming. However, specific processes, systems or individuals may cause incidents and accidents inadvertently, as well as intentional obstruction and attacks. Such knowledge alludes to the training of all entities involved in providing critical infrastructure protection. Although protection and "resilience" are critical infrastructure complementary concepts, different explanations should be elaborated on and accepted. In short, protection is a relation between the ability to prevent or reduce the effect of unpleasant and sudden effects. At the same time, resilience is manifested through the ability to reduce the magnitude, stiffness and duration of stagnation, and relationships rapidly access all components and processes, from physical components and the quality of human resources. Crucially, this paper would like to point out elasticity as the intention to develop and maintain a system and its ability to quickly prevent, absorb, adjust and recover from any possible attack. In security, resilience refers to various factors that indirectly contribute to and strengthen security. In the areas of critical infrastructure protection, "resilience" should be understood in terms of increased security, identification and application of measures that may be required at critical infrastructure levels, but especially at the organisation and process levels that provide access or use outputs. Such assumptions alert and require an urgent reaction from the called-upon national institutions to take concrete steps. This means defining and strengthening social resilience, protecting critical infrastructure through the construction of a system and the eventual implementation of the critical infrastructure resilience concept. In this paper, the authors will pay special attention to the analysis of contemporary challenges for the Republic of North Macedonia in terms of geopolitics, threats of terrorism, hacker attacks and other hybrid threats, new technologies, and climate change and security.

Changing the nature of the global geopolitical and security landscape

We can start with the statement that the World is experiencing a turning point in the second decade of the 21st century, marked by a geopolitical and economic shift of power from the West to the Eurasian powers. The current period brings various geopolitical and geostrategic challenges, which are certainly more specific to deal with than those in the 20th century. These challenges include political confrontation, internal and international political conflict, and conflict over natural resources in war-torn civil countries across sub-Saharian Africa, Latin America, the Middle East, and the newly explored strategic regions, such as the Arctic. The rapidly expanding progressive population of the World is facing cyclical fluctuations in food prices due to climate change, economic conflicts, the rise of religious fundamentalism, and the fragmentation of the World's political map.

We are rightly faced with the dilemma of whether the 21st century will be defined by rivalries between national (super) powers and not by the supremacy of collective systems or overlapping sovereignty, replacing sovereign states as New Medieval theorists and conspirators expect. Which will be the dominant force in the multipolar World - the rapidly weakening United States, on the one hand, or the even more secure China, which is seeking to restore its status as the most robust economy in the World? (Riegl and Landovský, 2013).

These global trends create the World's geopolitical landscape. The World is redefining its geopolitical patterns and principles in the second decade of the 21st century. The euphoria with the end of the Cold War, enshrined in Francis Fukuyama's concept of the end of history, was premature. The clash of 21st-century civilisations would not define the geopolitics of the 21st century. It is Europe that, unfortunately, reflects the geopolitical violations on the political map. The map of Europe defines the 21st century. From the fields of Flanders (World War I) to Omaha Beach (World War II) to the Berlin Wall to the burned villages on the territory of the former SFRY, from the lengthy European war of 1914 to 1989, to the current bloody war aftershocks in Ukraine, Europe is the centre of world geopolitics and history. (Riegl, 2013).

The geopolitical transition of power from the Euro-Atlantic to the Asia-Pacific region (especially from the United States to China) is continuing. It has been confirmed by geopolitical analysts such as Nye, Brzezinski, and Kaplan.

Joseph Nye identifies five significant global challenges (including possible reactions) in response to the most pessimistic projections of US decline and the inevitable rise of China's economic and geopolitical dominance.

He discusses the challenges in promoting the American strategy for smart power in his book "Future of Power". Describing the strengths and limitations of American power, Nye explains that the smart power strategy seeks to bridge the old gap between liberal and realistic needs, leaving room for a new synthesis called liberal realism. In the context of smart power it is not the creation of an empire or hegemony. The United States can influence, but cannot control, all parts of the World. Power depends on the specific context and the context of transnational relations (climate change, drug trafficking, pandemics and terrorism), and it is diffuse and chaotically distributed. Military power plays a small role in resolving and responding to emerging threats. Responding to these threats requires more cooperation with governmental and international institutions. Nay also emphasises that the liberal realist strategy emphasises the importance of developing an integrated "big" strategy that combines hard and soft power into smart power. In the fight against terrorism, the United States should use strong force against hardline terrorists, but no victory can be expected until it is won in the hearts and minds of Muslims. Furthermore, the liberal realist strategy aims to provide security for the United States and its allies, maintain a strong domestic and international economy, avoid environmental catastrophes, and strengthen liberal democracy and human rights at home and abroad.

Five major challenges provoke Nye's new strategy. The first challenge is to tackle terrorism with nuclear materials. This will require policies to counter-terrorism, create stability in the Middle East, give due attention to failed states, and so on. The second challenge is political Islam. According to Nye, the current struggle against radical Islam is not a "clash of civilisations", but a civil war within Islam. More open trade, economic growth, education, development of civil society institutions and gradual increase in political participation. The third challenge is the rise of hostile hegemony as Asia gradually regains its share of world economy. This challenge requires a policy that welcomes China as a responsible and vital entity, but protects against possible hostility by maintaining close relations with Japan, India, and other Asian countries that welcome the US presence. The fourth challenge is economic depression. The strategic response to this challenge will require policies that will gradually reduce US oil dependence, especially in the Persian Gulf, where 2/3 of the World's oil reserves are located. The fifth challenge is environmental crises, such as pandemics or adverse climate change. This challenge requires prudent energy policies, leadership in the field of climate change and greater cooperation within international institutions. (Nye, J.S., 2011: 231-233).

In his book "Strategic Vision: America and the Crisis of Global Power", Zbigniew Brzezinski tries to answer four significant dilemmas.

1) What are the implications of the changing distribution of global power from West to East,

2) Why is America's global appeal weakening, what are the symptoms of America's domestic and international decline, and what geopolitical reorientation is necessary to revitalise America's global role?

3) What would be the likely geopolitical consequences if America relinquished its globally prominent position, what would be the almost immediate geopolitical victims of such a decline, what effects would it have on the global problems in the 21st century, and could China take on America's central role in world affairs by 2025?

4) Looking after 2025, how should a resurrected America define its long-term geopolitical goals, and how can America, with its traditional European allies, try to engage Turkey and Russia to build an even bigger and more energetic West?

Brzezinski offered a strategic vision for the so-called Greater West, which stretches from Vancouver to Vladivostok, and the cooperating east. The Greater West will include rapidly developing Turkey and Russia. The two countries will be integrated into the Euro-Atlantic institutional design, stretching from Vancouver to Vladivostok in the Far East.

The ultimate goal of the more prominent and vital West in working closely with Europe must be accompanied by a strategy of a stable and cooperative East. The success of this strategy lies in the successful moderation of the Chinese geopolitical concerns, which are the following:

1) To reduce the dangers inherent in China's potential geographical environment due to: US security links with Japan, South Korea and the Philippines, vulnerability to China's naval access to the Indian Ocean via the Malacca Strait and beyond to the Middle East, Africa, Europe,

2) To establish for itself a favoured position in the emerging neo-linguistic community and also in the already existing ASEAN,

3) To consolidate Pakistan as a counterweight to India,

4) To gain a significant advantage over Russia in economic influence in Central Asia and Mongolia, thus partially meeting China's natural resource needs, also in areas

closer to China than Africa or Latin America, to resolve China's remaining unresolved legacy of the Taiwan Civil War,

5) To establish a favoured economic and indirect political presence in several countries in the Middle East, Africa and Latin America. (Brzezinski, 2012).

However, the geopolitical battle for power will be fought in a political and geographical area different from the last century. Europe has ceased to focus on geopolitical and geostrategic considerations of key actors. Robert Kaplan predicts that the battle will shift from the European coast to the east.

According to Kaplan, the Great Indian Ocean, which stretches east from the Horn of Africa along the Arabian Peninsula, the Iranian highlands and the Indian subcontinent to the Indonesian archipelago and beyond, could be an iconic map for a new century like Europe to the last. We can locate the tense dialogue between Western and Islamic civilisations, the ganglia of global energy routes, and the quiet, seemingly unstoppable domination of India and China over land and sea. (Kaplan, 2010).

In such previously described world geopolitical constellation position of the Western Balkans and from the perspective of North Macedonia, one gets the impression that the region and the country have been turned into a geopolitical laboratory. In that laboratory, geopolitical experiments find applications in creating the geopolitical landscape in the Western Balkans region. Let us look only at the policies of the EU enlargement. The recent events allude to the fact that North Macedonia must accept everything, primarily to its detriment, to step on the European path. Something that is not provided in the basic guidelines and preconditions for EU membership. Hence, we will point out several possible scenarios to bring sound conclusions and forecasts for what awaits North Macedonia on its path of the enlargement process.

Scenario 1. The European Union is moving from the principle of unanimity to a qualified majority in decision-making on enlargement. In this way, if North Macedonia starts to reform with significant results, it will be a good argument for EU member states for the country's capacity to meet the requirements set out in the new enlargement methodology. The EU process for North Macedonia will be open with a qualified majority.

Scenario 2. For economic gain, membership in the European Economic Community (EEA), but without political unity. A long pause in the enlargement process until 2030, and in the meantime, the strengthening of the European Neighborhood Policy, which does not include accession, has offered privileged partnerships.

Scenario 3. Without serious EU efforts to integrate the Western Balkans, the region is moving towards Chinese hegemony and possibly Russian destabilisation. The pandemic and the crisis of American democracy have shown us that the West is not recovering democratically. Further analysis shows the possible transition to at least binary US-Chinese hegemony and Chinese hegemony in the long run.

Scenario 4. Stagnation of the enlargement process and putting the Balkan countries in uncertainty, with the option of a “mini-Schengen” zone.

Scenario 5. Return of US diplomacy to the Balkans, assisted by German diplomacy or return of so-called "bulldozer diplomacy" to close open disputes in the Balkans, but with possible adverse effects, in the long run, after the EU project. (Mileski and Klimoska, 2021).

Hybrid threats and hybrid warfare

In the 21st century, hybrid threats are becoming a dominant security challenge for Western nations and their critical infrastructures. Their appearance reflects a significant change in international relations. Due to the complexity and ambiguous nature of hybrid threats, such a change tends to increase feelings of insecurity and, historically, to increase dissent in societies. In such a situation, some people look for answers in the past, while others forget the past. Some trends advocate adaptation to emerging conditions and change, and some try to defend the so-called status quo. All these perceptions indicate that the image of the security environment is not just black or white. It is complex, multilayered and multidimensional. Hence, a proper analysis of what has changed, how it is changing and what it means for democracies is at the core of understanding the nature of the current security environment in Europe and the World.

Regarding Treverton, six significant changes bring hybrid threats to the forefront. The first is the changing nature of the world order. Modern developments indicate that relational power - the power to change other people's beliefs, attitudes, preferences, opinions, expectations, emotions and/or predispositions to action - is more critical today than material power. This change is used by the great and middle powers to increase their international status and gain certain benefits.

Second, the World sees a new type of network-based action or the dark side of globalisation. The internal and external dimensions of security are more closely interlinked than in recent decades. The role of the nation-state is questioned, as is the role of alliances with several norms and rules that limit responses to asymmetric and antagonistic actions.

Third, rapidly evolving technologies, their literal revolution, are challenging new domains such as cyberspace, where national and international game rules have yet to be created. Space is no longer a border, but an operational empire, which is also a challenge to traditional security thinking. In general, new technology provides new tools for influence.

In particular, the changing domain of information space and media landscape is the fourth significant change affecting today's security environment. Digitalisation and social media, as new creators of thought, have changed the speed at which information travels, how information is produced, and how people connect across national borders. This change has fueled the need to understand different political and strategic cultures because information produced in one country can be interpreted differently elsewhere. Information custodians are also changing. The Internet has become a new battleground where rules are still being formulated. False news, content confusion and "facts" based on certain opinions agitate the public. Trust, one of the basic pillars of functional societies, is increasingly eroding.

The fifth change is the changing nature of conflict and war. In today's wars, soldiers should not die, and civilian casualties should be avoided. This finding has led to a debate about the blurred lines between war and peace. The situation with the blurred lines between war and peace is highlighted and poses a challenge to conventional military forces and internal law enforcement. It also fosters hybrid threats, which try to stay under open conflict. They are more and more like competitions between societies, not armies.

Finally, the sixth change refers to the change of generations. This means we have left behind the Cold War and even the post-Cold War era. The Cold War had two very different characteristics which maintained the world order: the relations of the superpowers and their ideological struggle between communism and capitalism dominated. At the same time, the fear of nuclear war guided many security policy decisions. During the post-Cold War era, globalisation, emphasising the ideas of integration and interdependence, became a modern way of describing the World. Today's new generation is a digital generation informed by two contradictory trends - cosmopolitanism and neo-nationalism. Historical memory also changes with the generations, which leaves room for political manipulation of historical events. (Treverton et al., 2018).

On another side, Frank Hoffman defines hybrid warfare as a series of different forms of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal activity. (Hoffman, 2007: 14). Supposing the critiques of the definitions of hybrid wars were mainly based on the reliance on non-state actors. In that case, Hoffman puts his definition by saying that hybrid wars can be conducted by both warring states and by different non-state actors.

One of the most comprehensive definitions of hybrid warfare is offered by Najžer. Namely, he emphasises that hybrid warfare is a unique form of low-level conflict that encompasses many capabilities. It is a deliberate covert fusion of conventional and unconventional warfare conducted under a single central government and led by a state or non-state actor. Hybrid warfare aims to achieve political goals that would not be achievable or would be too costly through any other form of warfare. The mix of the conventional and the unconventional allows the actor to exploit the strategic or doctrinal weakness of the opponent while maintaining the denial of involvement in the conflict and the strategic surprise. (Najžer, 2020: 29).

Terrorism as a hybrid threat

The changing nature of terrorism as a hybrid threat can be understood if we accept the conclusion that the end of the 20th century and the beginning of the 21st century is a critical period in the history of security when there is a rapid transition from an analogue to a digitalised globalised world. In such an environment, there comes the transformation of terrorism, or as Antinori puts it, the "media morphology of terrorism". This process is a transformation in which the media are not only sources of information that generate terror, as provided by traditional propaganda strategies. The media generate terror as an asymmetric threat to the globalised contemporary reality through violent nexus: action-presentation.

Terrorism is taking on new methods and applying new environments. Theorists become e-theorists and apply "cyber terrorism", emphasising technology's role in the attack, digital terror and (cyber) social terrorism using social networks. (Antinori, 2019: 24).

Terrorism is one of the greatest threats that must be highlighted in all hybrid threats. Terrorists operate simultaneously in many countries, using deadly methods against European Union and NATO member states. In addition, all terrorist attacks hinder global cooperation in carrying out civilian and military missions to stabilise the host country's situation. The absence of timely action leads to the destabilisation of the situation in many countries.

It must be borne in mind that terrorist organisations, which are also perceived as "hybrid actors", can achieve real operational success by controlling large-scale territorial expansions in Syria and Iraq. In addition, the active presence of terrorists on social networks for propaganda is also an essential element of the hybrid activity. (Olech, A. 2021).

The changing nature of terrorist activity is becoming increasingly relevant in the efforts to build resilient societies and the need to build effective systems to protect critical infrastructure.

Hacker attacks and technologies that undermine the security

With its development, we live in a world where the Internet contributes to the online business making significant progress. The rapid development of the Internet has led to tremendous benefits such as e-commerce, email and easy access to vast amounts of data. This means that more and more computers are connecting to the Internet, wireless devices and networks. For these reasons, due to the innovative benefits of the Internet, the administration, the private industry and regular computer clients are increasingly concerned. And the fear of possible criminal hacking of their information or private data.

Hacking is the unauthorised use of computer systems. Hackers are programmers who bypass security systems, hack into someone else's computer or collect information without authorisation. (Kumar and Agarwal, 2018).

Critical infrastructure is not immune to this type of attack. Despite security systems, numerous examples of unauthorised outages and damage to critical infrastructure. The main features of hacking can be: unauthorised access to the information system, forced hacking or access to the security system, high professionalism and knowledge to achieve the intrusion of the system; usually, the place of attack is far from the place of the attacker, the scope of a hacker attack can also be spying, fraud, embezzlement, theft of services, sabotage, spreading viruses, hackers usually act in groups or individually. As a result of such actions, especially in critical infrastructure, various consequences are possible, such as disruption of the protection system, blocking or slowing down the normal functioning of systems, unauthorised access, damage, modification or destruction of data, theft, illegal distribution of malware or the spread of viruses.

Analogous to the previous findings, the technological advancement provided by the 5G network has unique possibilities for practical use. The term 5G denotes the 5th generation of mobile telecommunications, the main feature being the speed of data transfer and the contents of the massively connected devices. Every global technical-technological innovation, in addition to the additional ones, also hides opportunities for abuse and use of technology that undermine security.

Critical infrastructure, defence, and security are not immune to the potential threats of 5G technology. The West's controversies and general attitude regarding the withdrawal or ban of Huawei, the technology giant from China, are known. The potential dangers of this technology, where the Chinese Government, through its control of the wireless and telecommunications pillar in the World, will use 5G technology such as a Trojan horse for commercial and military purposes or espionage and hybrid warfare. (Evans, 2020)

In technologies that undermine security, we can classify the increasing use of drones. Interestingly, these innovative technologies are associated with the term "grey zone" and the strategic landscape that will increasingly portray challenges in the grey zone that are neither total war nor complete peace. RAND Corporation defines the grey area as a functional space between peace and war, which includes coercive actions to change the status quo below the threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military action. In the Center for Strategic and International Studies (CSIS) publications, the grey area strategy is defined as an effort or series of deterrents and assurances outside the steady state that seeks to achieve its security goals without resorting to direct and effective use of force. By engaging in the grey zone strategy, the actor tries to avoid crossing the threshold that results in war.

The changing nature of warfare, the strategy of hybrid wars, hybrid threats, proxy and cyber warfare allow more frequent use of drones. Military drones are actively used for operational use in two missions: reconnaissance and targeted killings. In doing so, their unique unmanned functions are helpful in such missions. In addition, drones are considered less expensive in terms of international reputation. (Hwang, 2021).

This development further increases the vulnerability of critical infrastructure. Particular targets for drone strikes may include fuel or water storage plants, pipelines, power distribution plants, and food supply sites with minimal or no staff. (Pledger, 2021). This means that even in that domain, the resilience and protection of critical infrastructure must be constantly upgraded and improved.

Climate change

Today, the World lives in a dynamic time where the intensity and catastrophic consequences of changes in the field of the environment impose the need for serious observation of natural events. They are more and more often manifested and more and more seriously endanger the security of the states and individuals, but they also affect the protection of critical infrastructure.

In a changing international constellation of conditions, relations and processes, climate change is a phenomenon that ranks high in political and academic debates. However, what is the nature of climate change? How do they affect and threaten critical infrastructure, and how do they generally model relations between countries, regions and the entire international community?

Unlike traditional strategic security concepts related to military action, climate change highlights how human security is at stake and how actors can take advantage of or force environmental change to undermine opponents. It has been written since the time of Sun Tzu that creating vulnerability in the opponent is too expensive, except for taking advantage of environmental factors. It is evident that, in the twenty-first century, we also see opportunities for asymmetric action against adversaries by opening up to environmental vulnerabilities. (Briggs, 2020).

For instance, the answer to the modern challenges of climate change in the energy sphere should be in the synergy between improving the resilience of the energy-critical infrastructure to extreme climate events and the transition to energy with less carbon. Paying for and restoring climate damage could jeopardise the financing of the transition to renewable energy and other low-carbon measures. Financing the transition to clean energy in the face of growing climate change will require creative options from policymakers and businesses. Innovative public-private structures will need to be considered when finding options for climate adaptation of energy systems. (Ogden et al., 2019)

A Case Study: North Macedonia

Macedonian society is not exempt from global political, security and economic currents. Macedonian society is in a starting position regarding the protection of critical infrastructure. It requires, before establishing the strategic and national framework for ensuring effective steps towards building an efficient system for the protection and resilience of critical infrastructure, to choose the approach to the optimal model and start its implementation. The optimal model based on the best practices of the “voluntary” and “mandated” approach in protecting critical infrastructure should be built on other countries’ good practices and experiences. Considering that the beginning of the construction of the critical infrastructure protection system is already late, the comparative and analytical approach is set as a top priority in order to start decisively creating the preconditions for fulfilling the concept of protection and resilience of critical infrastructure and with that, greater resistance of the Macedonian society.

At the beginning of creating social resilience, protection and resilience of critical infrastructure, we must know what to achieve. The EU model (Directive 2008/114/EC) is more protection oriented, although, since 2012, social resilience (resilience of communities) and resilience of critical infrastructure have been increasingly mentioned. It should be noted that there are other models, such as the Nordic model, where resistance to vital social functions is the main priority. In the organisational and technological domains, this Nordic approach is more visible in social resilience, where the key players are the national and local authorities. Regarding critical infrastructure operators, the concept of resilience is still quite abstract and has no concrete operationalisation. The open dilemma remains that the interaction between authorities and critical infrastructure operators, whether discussed in terms of regulation, state support, public-private partnership or corporate social responsibility, persists as a weak link in achieving critical infrastructure resilience in practice. The big question is whether it can be achieved at all. A review of the Nordic countries' conceptual approaches to critical infrastructure crises nevertheless gives the impression that these countries are pretty "progressive" and have always had a broader and more holistic philosophy than the one initially offered by the European Commission, based on the priority of critical infrastructure protection. (Pursiainen, C. 2018)

Analysing numerous literature (Mottahedi et al. 2021) and placing it in correlation with the changing strategic environment, hybrid threats and new technologies that undermine security, we can offer a unique model for building a comprehensive system for the protection of critical infrastructure in North Macedonia. This means constantly upgrading social resilience, establishing a CI protection system and upgrading the existing models with what we have called the concept of critical infrastructure system elasticity. In doing so, we mean reducing the recovery time of the CI systems or returning to the pre-disrupted state. Hence, social resilience and protection should be a function of the CI system resilience.

Possible model of CI protection and resilience

Strategic framework. It analyses the approaches and models for protecting critical infrastructure and the knowledge that critical infrastructure is a platform for maintaining the development of every society and state. The state government should be included in the system of protection of critical infrastructure as a proposer of laws and bylaws and has the task of authorising certain ministries to be coordinators of the whole system. The Government provides a strategic framework that is essential for the successful functioning of the system, cooperation, communication and coordination of all actors involved. The Government also designates (by separate decision) the sectors of certain critical infrastructures to provide a holistic approach to the protection and mitigation of negative impacts in the event of a threat to critical infrastructure.

After the Government, the next most important factor is the coordinator (a specific ministry) of the entire system to protect critical infrastructure. There are various examples and practices regarding which body is appropriate for this role. In many European countries, the post is assigned to the Ministries of the Interior. Hence, different solutions and practices exist, but each country should recognise the most appropriate model. From the comprehensive analysis, it can be suggested that the Ministry of Defense or the Ministry of Interior be the coordinator of the entire critical infrastructure protection system. If the MoD/MoI is the coordinator of the system, it will communicate directly with all system and international actors and submit reports to the Government. An organisational approach to the implementation of critical infrastructure protection in the European Union and countries aspiring to full membership (such as the Republic of North Macedonia) is given in Directive 2008/114 / EC on the identification and designation of critical European infrastructure and the assessment of the need to improve their protection - a vital document of the European Union for critical infrastructure. In order to be able to take a decisive step towards the implementation of the above, a few initial recommendations are useful for policymakers:

First. Proposal for preparation of a Strategy for the protection of critical infrastructure as a separate strategic document. This strategy should be a synthesis of decisive and binding views that are closely related to the protection of critical infrastructure. The commitments should address current and future security challenges and threats at the national, regional and broader levels, independently and in cooperation with allies and partners within the Collective Security Systems - NATO. However, the strategic solution should be a framework that determines the development component and the role of all entities in strengthening the protection of critical infrastructure and its resilience. A separate strategic solution would be a longer-term and more comprehensive option than updating certain strategic documents that would shorten the time to start specific activities.

Second. Under the assumption that a need has been identified to review the existing or develop a new national security strategy, it is necessary to devote space to the critical infrastructure in the strategy. It is undisputed that the National Security Strategy should include a section on critical infrastructure. The factual situation indicates that the critical infrastructure is mentioned in the 2020 Defense Strategy.

Namely, the Defence Strategy derives from the Constitution of the Republic of North Macedonia, the permanent provisions of the National Concept for Security and Defence, the Law on Defence and the strategic commitment of the Government of the Republic of North Macedonia to integrate into the Euro-Atlantic structures. Critical infrastructure is mentioned as one of the greatest threats to national security.

Third. If a Cyber Security Strategy exists or is in the process of being developed, critical infrastructure may be mentioned. Such a strategy was prepared in 2018, and it has parts that are aimed at protecting the critical information infrastructure as part of the overall critical infrastructure. An Action Plan for protecting critical information infrastructure has also been adopted. (National Cyber Security Strategy of the Republic of Macedonia, 2018-2022). Protecting the critical infrastructure is recognised and stated as a strategic goal within the National Strategy of the Republic of Macedonia for the fight against terrorism 2018-2022. (National Counter-Terrorism Strategy BPT, 2018).

Normative framework. Normatively, a law on the protection of critical infrastructure could be proposed. Until it passes all the envisaged stages for its adoption, the topic of critical infrastructure may be temporarily regulated by another law or bylaw. (it is assumed that the procedures for this are shorter, and the problem can be temporarily fixed faster).

When drafting the critical infrastructure regulations, the recommendation is to regulate the energy and transport areas primarily - the European Union requires these two segments from its member states and those who intend to join. If the other sectors of the critical infrastructure are involved, the experience of Croatia can be repeated at the very beginning to slow down and complicate the process. Therefore, it is recommended to start with the energy and transport sectors. The possibilities for regulating critical European infrastructure should be foreseen in the forthcoming normative solutions (law and bylaws).

It is especially important to state the security coordinator in the law or bylaws, who is a key figure in all bodies and organs which will be in charge of matters related to critical infrastructure. The Minister determines who will be the Security Coordinator for Critical Infrastructure in his/her ministry. In contrast, the Director General of the facility designated as Critical Infrastructure determines who will be the Security Coordinator. Experience shows that there are study programs that train staff for security coordinators. Such is the case in Romania, which allows individuals to be trained as security coordinators and seek employment in ministries or critical infrastructure facilities. If this example is followed, in addition to creating and accrediting such study programs, it is necessary to include a new work post of a security coordinator for critical infrastructure in the job classification in the country.

Furthermore, the place or role of public-private partnerships should be emphasised in the law or bylaws. This is extremely important as part of the critical infrastructure is operated by private companies. The 2020 Private Security Act does not contain any benchmarks related to critical infrastructure.

An essential segment in the law or bylaws should be the emphasis on schooling, education and training.

Organisational framework. The organisational aspects of implementing the measures and activities for protecting critical infrastructure should belong to the newly established Critical Infrastructure Protection Centre. For these reasons, the Ministry of Defence or the Ministry of Interior may be an excellent choice to be the state coordinating body for this process. This is because the Centre should collect data and coordinate activities. It is also important to state in the law or bylaws that the work on protecting critical infrastructure will take place through the Critical Infrastructure Protection Centre.

It is very important to avoid blocking the process from the beginning. The secrecy marks at the beginning should be the lowest possible. In creating strategic and legal solutions, an inter-ministerial group should be formed, including a wider circle of experts, from universities, ministries, chambers, and the private sector. After adopting the law, it is further necessary to regulate the individual processes with bylaws.

Following the adoption of the strategy and the law, it is necessary to start constructing the critical infrastructure protection system. It is important to note that the system is built with the help of education, workshops and learning all the factors in that process. Optimally, we would point out the need to create a five-year action plan. (Mitrevska et al. 2019).

Conclusion

The previous findings conclude that Macedonian society is late in creating an efficient critical infrastructure protection system. The intensity of adverse events, natural or anthropogenic, empirically shows that even more developed societies face problems in establishing effective critical infrastructure protection systems. The personal experience of other countries indicates that analytically and comparatively, we can draw solid benefits and timely prevent any shortcomings in the construction of the protection system.

From the very beginning, the complexity of the wide range of sectors within the critical infrastructure indicates the realisation that the process of building the system is long and laborious. If this is followed by the complexity of the policies for critical infrastructure protection and the latest trends in applying the concept of resilience, we may conclude that the newly established dynamics of risks and threats require new responses from the security systems. This means establishing new institutions within the security system that, as their integral part, with an interdisciplinary approach, will analyse the latest trends in risks and threats according to different criteria. Traditional elements of security systems would not be very effective in dealing with modern risks and threats, especially cyber threats and the like. Hence, space must be allowed for scientific institutions, the private sector and several other entities that directly or indirectly contribute to critical infrastructure work.

The Macedonian critical infrastructure protection system must be based on the model in development and, at the same time, integrate the concepts of social resilience, protection and elasticity of critical infrastructure. It may be too ambitious initially, but it is better to keep in mind the latest trends in developing critical infrastructure protection systems from the outset. Only in this way is a modern, resilient society amenable to development through the efficient functioning of critical infrastructure. This includes networks for the uninterrupted provision of public services, improving the quality of life, and maintaining private profits and economic growth.

REFERENCES:

Antinori, A. (2019). Terrorism and DeepFake: From hybrid warfare to post-truth warfare in a hybrid world. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics. Academic Conferences and publishing limited;

Briggs, C. M. (2020). Climate Change and Hybrid Warfare Strategies. Journal of Strategic Security, 13(4), 45–57. https://www.jstor.org/stable/26965517;

Brzezinski, Z. (2012) Strategic Vision: America and the Crisis of Global Power. New York: Basic Books;

Evans, V.C., (2020) Future Warfare: Weaponising Critical Infrastructure. Parameters 50, no. 2. doi:10.55540/0031-1723.1017;

European Commision (2020). Proposal for a Directive on the resilience of critical entities. https://www.europeansources.info/record/proposal-for-a-directive-on-the-resilience-of-critical-entities/ (Accessed on 21.05.2022);

Hoffman, F. G., (2007) Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, December 2007;

Hwang, W. J. (2021). How are drones being flown over the gray zone?. Defense & Security Analysis, 37(3), 328-34;

Kaplan, R.D. (2010) Monsoon: The Indian Ocean and the Future of American Power. New York: Random House;

Kumar, S., Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. International Journal of Advance Research in Computer Science and Management, 4(4), 2253-2257;

Mileski, T., Klimoska, K., (2021) “France’s Geopolitical Vision for Europe and the Western Balkan: The Case of North Macedonia”. The Review of International Affairs. Vol. LXXII, No.1181, January – April 2021 DOI: 10.18485/iipe_ria.2021.72.1181.2;

Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: a systematic literature review. Energies, 14(6), 1571;

Mitrevska, M., Mileski, T., Mikac, R. (2019) Critical infrastructure: concept and security challenges. Skopje: Friedrich Ebert Foundation;

Najžer, B., (2020) The Hybrid Age: International Security in the Era of Hybrid Warfare. London: IB Tauris;

Nye, J.S. (2011) Future of Power. New York: Public Affairs;

Olech, A. (2021). Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism. Institute of New Europe;

Ogden, J. M., Greenberg, M. R., Jaffe, A. M., Busby, J., Blackburn, J., Copeland, C., Law, S., & Griffin, P. A. (2019). CLIMATE CHANGE IMPACTS ON CRITICAL US ENERGY INFRASTRUCTURE. In Impact of Climate Risk on the Energy System: Examining the Financial, Security, and Technology Dimensions (pp. 32–43). Council on Foreign Relations. http://www.jstor.org/stable/resrep21839.6;

Pledger, T. (2021). The Role of Drones in Future Terrorist Attacks. Association of the United States Army;

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? International journal of disaster risk reduction, 27, 632-641;

Riegl, M., Landovský, J., (eds.) (2013) Strategic and Geopolitical Issues in the Contemporary World. Newcastle: Cambridge Scholars Publishing;

Riegl, M., (2013) Introduction: Geopolitical and Geostrategic Threats of the Contemporary World. In: Strategic and Geopolitical Issues in the Contemporary World. Newcastle: Cambridge Scholars Publishing;

Treverton, F. G., Thvedt, A., Chen, R., A., Lee, K., and McCue, M. (2018) Addressing Hybrid Threats. Swedish Defence University.