CRISIS PREVENTION AND CRITICAL INFRASTRUCTURE IN WESTERN BALKANS

by Vasko Popovski, Ledion Krisafi, Ana Nenezić, Sead Turčalo, Donika Emini, Aleksandar Kovacevic

April 2023

supported by

Visegrad Fund

Crisis prevention and critical infrastructure in Western Balkans

Acknowledgements: This project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

This project No. 22220222 was made possible through Visegrad+ Grant from the International Visegrad Fund.

supported by

Visegrad Fund

Impressum

Title: Crisis prevention and critical infrastructure in Western Balkans

Publisher: Institute for Democracy "Societas Civilis" – Skopje

Authors: Vasko Popovski
Ledion Krisafi
Ana Nenezić
Sead Turčalo
Donika Emini
Aleksandar Kovacevic

Design: Linija DOOEL Skopje

This publication is available at:

https://idscs.org.mk/en/2023/05/02/crisis-prevention-and-critical-infrastructure-in-western-balkans/

Abbreviations

ADC	Austrian Development Cooperation
AI	Artificial Intelligence
CER	Directive on Resilience of Critical Infrastructure
CI	Critical Infrastructure
CMC	Crisis Management Centre
DDoS	Distributed Denial-of-Service
DRM	Disaster Risk Management
DRR	Disaster Risk Reduction
EC	European Commission
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
GIS	Geo-Information Systems
ICTs	Information and Communication Technologies
IT	Information Technology
JRC	Joint Research Centre
NDMAs	National Disaster Management Authorities
NIS	Network and Information Systems
PDNA	Post-disaster Needs Assessment
SDGs	Sustainable Development Goals
Sendai Framework	Sendai Framework for Disaster Risk Reduction 2015 - 2030
SOPs	Standard Operating Procedures
UNDP	United Nations Development Programme
UNDRR	United Nations Office for Disaster Risk Reduction
UNEP	United Nations Environmental Programme
USA	United States of America
WB	Western Balkans

1. Introduction

Critical infrastructure systems are the backbone of societies and communities providing vital support and essential services for their functioning i.e. water, energy, transportation, and health, as well as contributing to the economic development, security, inclusion and welfare of their citizens contributing to leaving no one behind. They are complex, interdependent and interconnected systems and networks providing an essential foundation for contemporary sustainable and resilient development.

Critical Infrastructure is "the physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society."

Source: UNDRR Terminology
https://tinyurl.com/ycyjcfsr

Critical infrastructure systems are exposed and vulnerable to a broad palette of risks and threats including natural and human-made hazards, security risks, cyberattacks and physical attacks, that are eroding their structures and functions, exacerbating existing and creating new vulnerabilities. With the projected impacts of climate change, increased underlying risk drivers (e.g. environment degradation, unplanned and rapid urbanization, etc.), insufficient risk reduction mainstreaming, as well as the emerging risk and future threats to the critical infrastructure i.e. harmful cyber threats by terrorists, organized crime entities or by "*hacktivists*[1]", it is expected that this negative trend will increase seriously affecting the societies, national economies, businesses, communities and individuals.

In this context, during the period from 2000 to 2019, at the global level, 7,348 recorded disaster events were claiming 1.23 million lives, affecting 4.2 billion people and resulting in approximately 2.97 trillion USD in damages and losses. In the 21st century, the trend points to disasters taking fewer human lives, but

[1] *Hacktivists* are hacker groups that work together to achieve a certain objective. They are mostly political in nature, but, also, social activism, religious activism or anything else could be their motivation. As in V.S. Nageswara Rao Kadiyala, Ripon Patgiri, Chapter Seventeen - An investigation on socio-cybercrime graph, Editor(s): Ripon Patgiri, Ganesh Chandra Deka, Anupam Biswas, Advances in Computers, Elsevier, Volume 128, 2023, Pages 423-443. [Online]
Avialable at: https://www.sciencedirect.com/science/article/abs/pii/S0065245821000735

generating much greater damage and economic losses compared to the 20th century and most of these damages are losses related to critical infrastructure.[2] In this sense, at the broader regional level, *The Regional Snapshot of the aggregated data reported by Member Countries across the Europe and Central Asia region (2020)* shows that 18 countries reported disaster-related damages to 3,318 critical infrastructure facilities, while 14 countries reported 536 damaged facilities in 2019.[3] With regards to the climate change projected impacts, "according to JRC, annual damage to Europe's critical infrastructure could be ten-fold by the end of the century under business-as-usual scenarios due to climate change alone, from the current EUR 3.4 billion to EUR 34 billion." [4]

In addition, a *range of technical and technological disasters* are threatening the resilience of critical infrastructure e.g. the explosion and oil spill on the Deepwater Horizon platform in 2010 in the Gulf of Mexico, the collapse of the Ponte Morandi bridge in Genoa on 14 August 2018 or Beirut Port Ammonium Nitrate Explosion in 2020. The COVID-19 *pandemic crisis* impacted critical infrastructure in an unprecedented way shifting their operation to uncharted areas and with the main impact on the health sector while cascading across the other sectors (e.g. crisis management/civil protection, transportation, etc.), disrupting the global, regional and national supply chains and connections, as well as challenging their "operation and business continuity"[5] (e.g. availability or accessibility of resources).

Future risks and threats to critical infrastructure include examples of harmful cyber threats and attacks i.e. ransomware attacks (e.g. Deutsche Bahn suffered a massive service interruption when its systems were attacked by the global WannaCry epidemic of 2017, Danish transportation and logistics giant Maersk suffered $300M of business interruption losses due to the NotPetya outbreaWk of 2017[6], while Colonial Pipeline attack in 2021 disrupted nearly half the oil and gas supply for south-eastern of USA), dormant remote access software attacks (e.g. in February 2021 the Florida water treatment facility was hacked and the hackers tried to

---

[2] Santiago Lema-Burgos. Disaster Risk to Critical Infrastructure: Understanding critical infrastructure in the ECIS region. UNDP. 2019. p. 1.

[3] UNDRR—Regional Office for Europe & Central Asia. Sendai Framework Monitoring in Europe and Central Asia: A Regional Snapshot. December 2020. p. 19. [Online] Avialable at: https://tinyurl.com/69chscnd

[4] UCP Knowledge Network. Disruption to Critical Infrastructure (Web-article). 27 June 2022. [Online] Available at: https://tinyurl.com/yy352ft5

[5] Luca Galbusera, Monica Cardarilli, Georgios Giannopoulos. "The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures". Safety Science, Volume 139. 2021. [Online] Available at: https://www.sciencedirect.com/science/article/pii/S0925753521000047?via%253Dihub

[6] https://www.acronis.com/en-us/blog/posts/ransomware-logistics/

poison the water source), sabotage of the Nord Stream pipeline in 2022 or a series of DDoS attacks by pro-Russian hacktivists. Furthermore, in the case of the European Union, sophisticated hybrid attacks threatened cybersecurity and democracy by exploiting its vulnerabilities through a combination of cyberattacks and cybercrimes resulting in damages to critical infrastructure e.g. increased number of cyberattacks against cyber computers, healthcare and financial systems or hacking sensitive researches from medical organizations and pharmaceutical companies[7]. ICT threats have also been flagged as a key source of systemic risk to electoral processes and the EU financial system[8]. These events show a worrying acceleration towards asymmetrical virtual crime[9]. Considering the interdependency, interconnectivity and complexity of the world today, all of these global and regional experiences and practices apply to the Western Balkans economies and they are elaborated in the next section of the document.

Damages to the critical infrastructure as a whole or any of its sub-systems lead to structural failures, disbalance or disruption in the provision of services which ultimately hinder sustainable and resilient development. In that sense, all these

Resilience of the critical infrastructure system is defined as the ability to absorb, adapt to and/or rapidly recover from a potentially disruptive event.
Source: https://tinyurl.com/3axyputv

above-mentioned events underscore the fragility of critical infrastructure and emphasize the need for building its resilience through a systematic approach aimed at delivering resilient and reliable services. "Critical infrastructure systems need to be understood in their complexity and interdependency vis-a-vis sectors and subsectors as they incorporate key elements such as systems, assets, facilities, provision of services and human resource."[10] The critical infrastructure relates to crisis management and disaster risk reduction and building its resilience contributes to this relation. Namely, maintaining existing and investing in new infrastructure mitigate the adverse impacts of crises and disasters through better protection, and preparedness allowing for timely, effective and efficient response. On the other side, the availability and functionality of critical infrastructure are essential for timely and successful recovery enabling societies and communities to bounce back from these adverse events. Consequently,

[7] Craglia, M. et al., 2020, Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis. JRC Science for Policy Report, JRC121305.
[8] https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
[9] https://knowledge4policy.ec.europa.eu/changing-security-paradigm_en
[10] Vasko Popovski. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP. 2022. p.16. [Online] Available at: https://tinyurl.com/3hm772n4

societies and communities cannot be resilient without the resilience of the critical infrastructure and therefore the resilience-building approach is essential to be embedded into the risk-informed development of the countries and territories.

The purpose of this paper is to support the efforts for building the resilience of critical infrastructure to crises and disasters in the Western Balkans through the understanding of the overall critical infrastructure framework, an overview of the existing context in the six regional economies with recommendations for the way forward in building its resilience at the national and regional levels. In a consequent order, this brief aims to advocate for transformational change in understanding and applying the resilience-building approach in more effective ways to rethink their current approaches and upgrade the capacities and resources for better preparedness for existing, emerging and future unexpected crises.

2. EU and the resilience of critical infrastructure

The European Union embarked on the resilience-building of the critical infrastructure journey with the adoption of a policy framework and implementation of practical measures and actions. From the point of view of the former, the *Directive on the Resilience of Critical Entities* (2020)[11] aims to reduce the vulnerabilities and strengthen the resilience of critical entities[12] by creating an all-hazards framework to support the Member States in ensuring that critical entities can prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies. Furthermore, the NIS2 Directive on measures for a high common level of cybersecurity aims to respond to the same concerns for the cyber dimension, while the Digital Operational Resilience Act (2022) has an objective to strengthen the IT security of financial entities such as banks, insurance companies and investment firms. "Although the CER and NIS 2 directives are meant for the EU member states, they

[11] This Directive is replacing the 2008 Directive on European Critical Infrastructures.
[12] Critical Entitiy as per this Directive means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex.

should be open to candidate states obtaining observer status in the Critical Entities Resilience Groups and EU-CyCLONe."[13] Lastly, from the normative framework, there are the Council's Recommendations for a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (2022) which covers three priority areas: preparedness, response and international cooperation and proposes a more significant role for the Commission in tackling threats and enhancing interaction between the member states and third countries, particularly on infrastructure with cross-border relevance.

Regarding the supportive measures and actions, the EU launched the European Programme for Critical Infrastructure Protection for improving the protection of critical infrastructure in Europe, across all EU States and in all relevant sectors of economic activity and the Horizon2020 work programme includes a dedicated call for research on how to address combined physical and cyber threats to critical infrastructure. Furthermore, the JRC coordinates the European Reference Network for Critical Infrastructure Protection which carries out different research activities such as the development of methods and tools for international cybersecurity exercises and the Critical Infrastructure Warning Information Network provides an internet-based multi-level system for exchanging critical infrastructure protection ideas, studies and good practices. This initiative seeks to raise awareness and contribute to the protection of critical infrastructure in Europe.

In the context of the Western Balkans, the EC and representatives of the six countries in 2018 signed a Joint Action Plan on Counter-Terrorism for the Western Balkans which included certain regional and national actions regarding the critical infrastructure e.g. improved CI protection, improved protection of cyberspace and continued invitation of the representatives from the six economies to be part of the external dimension of EPCIP and its project and capacity development activities for CI protection.

[13] Denis Cenusa. EU Eastern Enlargement: Preparing for Current and Future Threats Through Inclusive Crisis Management and Resilient Critical Infrastructure (Web-article). SCEEUS Guest Platform for Eastern Europe Policy No. 21. 18 January 2023. [Online]
Available at: https://tinyurl.com/mrxtysuy

3. State of the play of critical infrastructure in Western Balkans

3.1 General Disaster Risk Profile of the Region

The region of Western Balkans has a complex regional risk profile with almost all natural and human-made hazards, climate change impacts, and high environmental degradation and pollution, coupled with the legacy of past conflicts and inter-ethnic tensions, as well as new and emerging security risks and threats. „Despite a strong rebound from the pandemic, the Western Balkans now face a new set of challenges, compounded by the war in Ukraine, including rising energy and food prices, high inflation, and slowing trade and investment."[14]

Table 1 - Risks and Hazards to critical infrastructure systems in the Western Balkans Region[15]

Natural hazards	Human-made & technological hazards	Security risks
• ***Geophysical*** (earthquake, landslides, mass movements, rockslides, mudflows, tsunamis) • ***Hydrometeorological*** (floods, flash floods, avalanches, drought, cold spells and heatwaves, severe convective and winter storms, wildfires, sea-level rise)	• Industrial accidents/pollution • Transport accidents • Large-scale power outages • Environmental degradation and pollution • Radiation • Dam failures	• Hostile governments • Terrorism • Proliferation • Cybercrime • Climate change • Transnational crime • Civil wars and wars • Untrusted investments • Population density • Supply chain attacks

[14] The World Bank. Western Balkans Face New Economic Headwinds Despite Strong Post-Pandemic Recovery (Press-release). 2022. [Online] Available at: https://tinyurl.com/32e5hy5e
[15] Vasko Popovski. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP. 2022. p.23. [Online] Available at: https://tinyurl.com/3hm772n4

• ***Biological*** (epidemics, epiphytotic, epizootics) • ***Cosmic phenomena*** (solar flares, geomagnetic storms, meteorites, asteroids)	• Factory explosions • Chemical spills	

From the natural hazards domain, floods are most frequent with the highest intensity and magnitude, wildfires are increasing in frequency and consequences for nature and biodiversity, other weather-related events are on the rise with greater magnitudes, while earthquakes have the potentially biggest impact in terms of loss of life and long-term damage and losses. For example, during the last two decades, there were 75 floods and 5 wildfire disaster events that resulted in 386 human losses, affecting 1.8 million population with a price tag in damages of more than 3.9 billion USD[16]. The magnitude of these disaster events on critical infrastructure systems in the affected WB countries can be identified from the post-disaster needs assessments conducted:

- Bosnia and Herzegovina Floods from May 2014 - out of the total audited impact of the floods of 2.4 billion USD, 30 per cent or 706.15 million USD were assessed damages and losses of the affected country's infrastructure systems, including facilities, assets and provision of services;
- Serbia Floods from May 2014 – contribution of the infrastructure damages and losses in the total assessed impacts of the floods (1.8 billion USD) is even higher i.e. 47 per cent or 854.22 million USD.
- Albania November 2019 Earthquake – damages and losses of the infrastructure sector were 14 per cent of the total disaster price tag of 1.19 billion USD.
- North Macedonia 2016 Skopje Flash Floods[17] - the ratio of damages and losses was 51:49 per cent or the impact on the infrastructure sector was audited as 18.7 million USD, whether the total price tag was 36.37 million USD.

This trend is expected to grow further given the expected impact of climate change that "will exacerbate extreme weather events in most areas of the WB region, particularly extreme drought- and heat-related events"[18] which can have an increased impact on the resilience of the critical infrastructure.

[16] https://www.ipaff.eu/floods-fires/#
[17] A PDNA Study was prepared but it was not officially adopted by the government.
[18] UNEP. Regional Strategy For Climate-resilient Road Infrastructure. ADC/UNEP. 2022. p.25. [Online] Available at: https://tinyurl.com/ys3j98er

Nevertheless, there are many examples of new and emerging risks and threats to the resilience of critical infrastructure in the region which required enhanced protection and anticipation by the government authorities and the owners and operators from the public and private domains. For example, the continuous migrant and refugee crisis resulted in most of the 1.4 million migrants and refugees that reach the EU transited to the Western Balkans Route[19], significantly pressuring the finite resources of the security and emergency management agencies and impacting the local communal and transport infrastructure. Furthermore, "the COVID-19 pandemic emphasized the absence of an adequate pandemic risk framework, expertise and related infrastructure"[20] and significantly pressed to the maximum the functioning of the health infrastructure sub-system, diverted funds from projects[21] to pandemic crisis response and overpressed the poor digital infrastructure in the six economies.

Future risks and threats to the security of critical infrastructure in the Western Balkans region include several events with intensified frequency and deepened impacts i.e. a series of cyber attacks on Albanian governmental and financial institutions' sites and portals during the summer and autumn of 2022[22], massive cyber attacks on Montenegrin online government information platforms placed the essential infrastructure, including banking, water and electrical power systems, at high risk in August 2022 or a series of similar events in North Macedonia e.g. DDoS attacks to the State Electoral Commission site during the July 2020 elections, email threats for placed bombing devices in 876 educational and 42 other institutions during the period October 2022 – March 2023 and ransomware attacks to governmental institutions e.g. Health Insurance Fund in February 2023.

Considering the current geo-political and security context in the broader region, the fact that the part of countries from the region is NATO member countries i.e. Albania, North Macedonia and Montenegro, as well as the continuous increase of cyber attacks, it is necessary to include these risks and threats in the policy and normative frameworks, risk and hazard assessments and plans and to design and apply adequate resilience-building actions and measures.

---

[19] Nermin Oruc, Saima Raza and Danica Santic. Analytical Report: The Western Balkan Migration Route (2015-2019). Prague Process Secretariat. March 2020. [Online] Avialable at: https://tinyurl.com/u4hbx9fz

[20] Vasko Popovski. Assessment Study of the Role of NDMAs in COVID 19 Crisis Response and Impact of Covid on NDMAs Operations. UNDP/UNDRR. 2020. [Online] Available at: https://tinyurl.com/3u3e5uey

[21] Ibid. p.41.

[22] Sulmet Iraniane, Artan Hoxha: Hakerat kanë marrë çdo gjë, edhe sistemin banker, Gazeta Tema, 11 Tetor 2022.

3.2 Critical Infrastructure Categorization

The departing point in the building of the resilience of the critical infrastructure to crises and disasters in the Western Balkan Region is the terminological definition and categorization. In that sense, it needs to be emphasized that theoretically, it is a new concept that emerged during the recent decades gaining its importance both from the complex disasters and crises i.e. 9/11 events in 2001 in USA or Madrid and London bombings in 2004 and 2005 respectively, as well as the sustainable and resilient global framework.

As a result of the former, the EC in the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection defines the critical infrastructure as *"an asset, system or part thereof located in the 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 on the Resilience of Critical Entities from 2020 modifies the understanding of critical infrastructure as *"an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service."*

Evolutionary, the critical infrastructure and building of its resilience in the WB countries appeared during the process of alignment with the global mechanisms and the accession process to the EU. The table below summarizes the definitions of the critical infrastructure systems in the Western Balkan countries and it can be seen that there is no uniform definition of critical infrastructure. In general, they are following the EU definition and refer to facilities, systems, networks or assets that are vital for the functioning of the countries' societies and systems or which interruption in the provision of services can threaten national security.

Table 2 - Definitions of the critical infrastructure in the EU and WB

Country	Definition
Albania	The physical structures, networks and other assets necessary for the economic and social functioning of a society or community. (Law on Civil Protection—45/2019)
Bosnia and Herzegovina (Republika Srpska entity)[23]	Systems, networks and facilities of particular importance, the destruction or endangerment which can cause serious disturbances in the free movement of people, transport of goods and provision of services, negatively affect internal security, human health and lives, property, environment, external security, economic stability and the continued functioning of state institutions. (Law on the Security of the Critical Infrastructure—2019)
Kosovo	Systems and assets, whether physical or virtual, are so vital to the Republic of Kosovo that the disruption, incapacity, or destruction of such systems and assets would have a debilitating impact on security, economy, public health, or any combination of those. (Law on Critical Infrastructure - 2018)
Montenegro	Systems, networks, facilities, or parts thereof located on the territory of Montenegro, whose interruption, i.e. interruption of deliveries of goods or services through these systems, networks, facilities, or parts thereof that may have serious consequences for national security, health and human life, property, environment, security of citizens and economic stability, i.e. performing activities of public interest (Law on designation and protection of the critical infrastructure—2019)
Serbia	Systems, networks, facilities or parts thereof, whose interruption in functioning or interruption in the delivery of goods or services, can have serious consequences for national security, health and the lives of people, property, environment, security of citizens and economic stability, that is, endanger the functioning of the Republic of Serbia. (Law on Critical Infrastructure - 2018)
North Macedonia[24]	Physical or virtual assets, systems, facilities, networks or their parts that perform vital functions of society, and which are of essential importance and the interruption of their work or their destruction would have a significant impact or serious consequences for national security, the health and life of people, the environment, the safety of citizens, economic stability, that is, the functioning of the state. (Draft-law on the Critical Infrastructure – Version December 2022)

[23] On a state level in Bosnia and Herzegovina, there is no accepted definition of critical infrastructure, but on the entity level, Republika Srpska has adopted a legislative act containing a definition of this term.

[24] In North Macedonia, the procedure for preparation and adoption of the Law on the Critical Infrastructure is ongoing and the definition from the current draft-version is presented for reference.

Another essential aspect of building the resilience of critical infrastructure is its categorization i.e., identification of key systems, assets, facilities and services that are considered to be critical for the country. Similarly, to the terminological definition domain, the countries from the Western Balkans follow the EU approach in this sense by acknowledging national contexts and differences. With the Directive on the Resilience of Critical Entities from 2020, there is the following categorization of the CI sectors and subsectors: energy (electricity, district heating and cooling, oil, gas, hydrogen); *transport* (air, rail, water, road, public transport); *banking; financial market infrastructure; health; drinking water; wastewater; digital infrastructure; public administration; space and production, processing and distribution of food.*

As can be seen from the table below, various approaches were taken in the identification of relevant CI sectors and sub-sectors, both following the EU approach and the national contexts and priorities. These categorizations of the critical infrastructure generally include "the energy, water, food, transport, telecommunications, healthcare, banking and finance sectors[25]" as the traditional core sectors for the functioning of the countries and territories. Most of them are "object-oriented"—this means that the particular physical assets/facilities or locations are considered within the individual sectors rather than "service-oriented"[26] with the integration of essential services that are provided by these sectors but can be considered vital for the societies and the communities. Another important aspect of the critical infrastructure categorization is the fact that most of the CI assets, facilities, resources and services are within the private domain i.e. they are privately owned or operated so it is crucial to balance this with adequate public-private-partnership mechanisms to secure their operationality and functionality. Nevertheless, the identification of the critical infrastructure is of great benefit in creating resilience-building policies and measures.

[25] Dr. Simone Sandholz. Five things you need to know about critical infrastructures (Blog). UNU-EHS. 2017. [Online] Available at: https://ehs.unu.edu/blog/5-facts/5-things-about-critical-infrastructures.html

[26] Vasko Popovski. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP. 2022. p.22. [Online] Available at: https://tinyurl.com/3hm772n4

Table 3 - Critical infrastructure sectors identified in the Western Balkans economies

Country	CI Sectors and sub-sectors
Albania	**Power generation, transmission and distribution systems; production, refining, treatment, storage and distribution of gas through pipelines; oil and production of its products, storage and distribution through pipelines; telecommunications** (networks, systems); **water supply; agriculture, production and distribution of food; public health** (hospitals, health centres and ambulances); **transport systems** (fuel supply, railway network, airports, ports, domestic transport); **financial services** (banking, clearing); **security and defence services.** (Law on Civil Protection—45/2019)
Bosnia and Herzegovina[27]	**Industry, energy and mining** (incl. input resources, facilities, transmission systems, storage, transport of products, energy and energy, distribution systems); **information and communication infrastructure** (electronic communications, data transmission, information systems, provision of audio, and audio and video media services); **traffic** (road, rail and air traffic and inland waterway traffic); **health care** (health care, production, transport and supervision of medicines); **communal activities, communal infrastructure facilities** (especially in the field of production and delivery water treatment, wastewater treatment and disposal, production and delivery of thermal energy, waste disposal from residential and commercial premisses, and more); **water management** (regulatory and protective water management facilities); **food and beverages** (production and supply of food and beverages, food and beverage safety system, inventories); **finance** (banking, stock exchanges, investments, systems insurance and payments); **production, storage and transport of hazardous materials** (chemical, biological, radiological and nuclear materials); **public services; education; cultural and natural assets** (religious buildings, cultural monuments, spatial cultural and historical units, archaeological sites, landmarks, works of art and historical objects, archives, film material, old and a rare book, as well as protected natural assets prescribed by the Nature Protection Act). (Law on the Security of the Critical Infrastructure—2019)
Kosovo	**Dangerous goods** (production and storage/processing of chemical, biological, radiological and nuclear materials); **energy** (production, transmission, distribution, storage); **financial services** (banking, stock exchange, payment and insurance systems); **food and agriculture** (production, processing, storage); **government institutional facilities; health care and public health** (health care, production of medical products); **information and communication technology** (electronic communication, video and audio broadcasting, information systems, telecommunication, data transmission); **national values; public services** (emergency services, protection and rescue, civil administration services, authorities government functions, postal and courier services, public order, justice and correctional service, armed forces); **transportation** (road, rail, air); **and water and wastewater** (supply, reservoirs and dams). (Law on Critical Infrastructure - 2018)

Montenegro	Energy; transport; water supply; health, finance; electronic communications; information and communication technologies; environmental protection; functioning of state bodies and other areas of public interest. (Law on designation and protection of the critical infrastructure—2019)
Serbia	Energy; traffic; water and food supply; health care; finance; telecommunication and information technologies; environmental protection and functioning of state bodies. (Law on Critical Infrastructure - 2018) [28]
North Macedonia[29]	**Energy** (production, including dams, mining, transmission, storage, transportation of energy and energy, distribution, etc.); **transport** (road, rail, air and water traffic); **banking systems and infrastructure of the financial markets; health** (health care, production, trade and control over medicines); water supply (water supply and drainage systems); **food** (food production and supply, commodity reserves); **production, storage and transportation of dangerous substances** (chemical, biological, radiological and nuclear materials); **public services** (ensuring public order and peace, protection and rescue, emergency medical assistance) **and digital infrastructure, communication and information technologies** (electronic communications, data transmission, information devices and installations, audio and audiovisual media services, etc.). (Draft-law on the Critical Infrastructure – Version December 2022)

[27] At the state level in Bosnia and Herzegovina, there is no accepted categorization of CI, but at the entity Level, Republika Srpska has adopted a legislative act which contains the category, critical infrastructure.
[28] There is an option with the law to identify infrastructure in other sectors if recommended by responsible Ministries.
[29] In North Macedonia, the procedure for preparation and adoption of the Law on the Critical Infrastructure is ongoing and the definition from the current draft-version is presented for reference.

3.3 Normative framework and institutional architecture for the resilience of critical infrastructure

As presented above, in four of the WB countries, there are legislative solutions on the critical infrastructure, in North Macedonia, this process is ongoing, whether, in Bosnia and Herzegovina, there is a relevant law only on the entity level (Republika Srpska), but not on the state level. In general, these legislative solutions are following the EU trajectory on critical infrastructure protection. They are providing definitions of the critical infrastructure, its categorization, essential protection, competencies and responsibilities of authorities, CI owners/operators and other entities, management and supervision, information and monitoring, reporting, etc. Nevertheless, the current approach is still "reactive", with the emphasis on the protection of the critical infrastructure sectors and sub-sectors, rather than "proactive" with the focus on prevention and mitigation as pillars of building their resilience.

Furthermore, besides this CI legislation solutions, some additional laws and by-laws are regulating certain sectors or aspects of the operation and functioning of the critical infrastructure. For example, in ***Albania***, there is a Law on the development of electronic communications networks[30], as well as the first-ever national Cybersecurity Regulation for the Electricity Sector. Furthermore, in 2017, the Albanian Parliament approved the Law on cybersecurity intending to achieve a high level of cyber security by defining security measures, rights, obligations and cooperation between the entities operating in the field of cyber security. Also, certain aspects are included in the National Civil Protection Plan, risk and hazard assessments, as well as sectoral plans, and some companies/CI operators such as the Electricity Distribution Operator and Trans Adriatic Pipeline, are preparing business continuity plans. In ***Bosnia and Herzegovina***, CI aspects are part of the national/local and sectoral strategies, as well as the risk and hazard assessments. For example, in the Development Programme of the Federation of Bosnia and Herzegovina for the period 2021 – 2028, specific DRR programmes and projects in the amount of 26

[30] As per this law, the Critical Information Infrastructure is the entire information networks and systems, the violation or destruction of which would have a serious impact on the health, safety and/or economic well-being of citizens and/or the effective functioning of the economy in the Republic of Albania and involves the energy, communication, financial and cybersecurity sector.

million USD are identified for the implementation of structural and non-structural measures for resilience i.e. increasing crisis resilience, ensuring the protection and functioning of the critical infrastructure and improving the functioning of the protection and rescue system. Considering the latter, the Risk Assessment of Natural and Other Disasters in Bosnia and Herzegovina (2011) includes some hazards and risks that may pose a threat to some of the infrastructure systems e.g. hazards in transportation and communication, industrial hazards, etc. Nevertheless, "laws on information/cybersecurity do not exist per se; rather there exists a patchwork of legislation containing elements that relate to the field, both in Bosnia and Herzegovina, as well as at entity-level and in Brčko District."[31]

In 2018 ***Kosovo*** adopted the law on critical infrastructure, but this legislative process was discontinued failing to develop the necessary secondary legislation which would build the necessary mechanisms, regulations, procedures, and institutions to make the law implementable. Considering the cybersecurity area, in 2022 it adopted the draft law on cybersecurity based on the NIS2 Directive with a main focus on the prevention of cybercrimes. In parallel, activities for the preparation of the new e-Government Strategy 2027 which places a focus on cyber security are ongoing. ***Montenegro*** is a specific case since it has adopted the CI law where security and safety plans for CI are defined, alongside the protection and rescue plans and risk and hazard assessments. Considering the cybersecurity area, the new Cyber Security Strategy 2022 – 2026 with an Action Plan 2022 - 2023 was adopted and in 2021, the Law on Information Security was amended partially transposing the NIS Directive (EU Directive 2016/1148).

From the legislative point of view, the situation in ***North Macedonia*** is specific, since the critical infrastructure law is under development, and the CI aspects are significantly mainstreamed in other acts, such as the Regulation of the integrated risk and hazard assessment. It provides a normative basis for the collection and analysis of data regarding the exposure and vulnerability of the infrastructure on the national and local level for risk and hazard assessment, operational and response planning) and the Regulation on the methodology for damage assessment in which an infrastructure inventory is included. On the other side, some of the infrastructure sectors are regulated by sectoral laws e.g. energy. And finally, in Serbia, besides the law on critical infrastructure, it is important to mention the Regulation on the criteria for the identification of critical infrastructure and the

[31] Geneva Centre for Security Sector Governance. National Cybersecurity Strategies in Western Balkan Economies. 2021. p.9. [Online] Available at: https://tinyurl.com/2p8w9bwa

method of reporting on the critical infrastructure, as one of the founding by-laws. The Information Society and Information Security Development Strategy for the Period 2021–2026 is a cross-sectoral strategy setting out the objectives of and measures for the development of information society and information security. Concerning information security, the Strategy is harmonized with the NIS Directive (2016). In light of the EU accession negotiations, Serbia, also, adopted the Strategy for Combating Cybercrime 2019-2023 which regulates the area of combating high-tech crime.

From the point of view of *institutional architecture*, the main competencies for the critical infrastructure are predominantly embedded within the structures of the countries' national disaster management authorities and they provide essential input for its protection. Based on the Law on Civil Protection in ***Albania***, the National Civil Protection Agency (Ministry of Defense) is responsible for its protection as well as for the critical infrastructure sectors with cross-border effects. In ***Kosovo***, the Ministry of Internal Affairs establishes a relevant institutional mechanism within its structure for the implementation of the critical infrastructure law and serves as the overall Contact Point for all national and European Critical Infrastructure Protection matters. In ***Montenegro***, the Ministry of Interior coordinates and monitor the implementation of the protection in a system where direct supervision is done by the sectoral ministries. Lastly, in Serbia, the Ministry of Internal Affairs regulates, plans, coordinates, controls activities, and communicates and provides information related to critical infrastructure. Following the planned transformation of the disaster risk management system and the incorporation of the Crisis Management Centre and the Protection and Rescue Directorate into the Ministry of Defense, the latter will be the main competent institution for CI once the draft law is adopted.

Nevertheless, there are many more in all phases of the risk reduction cycle that are emerging both from their capacities and resources, but also from the resilience-based concept, as well as many other actors that are part of the CI protection institutional framework and have competencies and responsibilities in their domains. Accordingly, the resilience-building of critical infrastructure is a multi-sector endeavour and various governmental institutions, authorities, organizations, private sector entities, academia, trade chambers and others are included in their roles and responsibilities. Almost in all countries, on the infrastructure facilities/services levels, the sectoral ministries are regulating and monitor the areas and the operators are responsible for their functioning/delivery, operations and maintenance, including the provision of the essential mitigation, preparedness, response and

recovery. Also, we can notice the decentralized approach where the local/municipal authorities are responsible for some of the critical infrastructure sectors on their territory with systems that are owned and operated by the local entities e.g., water/wastewater systems, and provision of related services.

In addition, the security of the critical infrastructure domain is managed by the institutions and bodies from the security area, whether the cyber security domain is managed by the relevant national authorities[32] i.e. ***Albania*** (National Cybersecurity Agency), ***Bosnia and Herzegovina*** (Ministry of Communications and Transport and Ministry of Security, whether at the entity-level: Federal Ministry of Transport and Communications and Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska), ***Kosovo*** (Ministry of Interior), ***Montenegro*** (Ministry of Public Administration and National Security Agency of the Ministry of Defence), ***North Macedonia*** (Ministry of Information Society and Administration) and in ***Serbia*** (Ministry of Trade, Tourism and Telecommunications).

[32] Geneva Centre for Security Sector Governance. National Cybersecurity Strategies in Western Balkan Economies. 2021. [Online] Available at: https://tinyurl.com/2p8w9bwa

4. Gaps and challenges in building the resilience of critical infrastructure in the Western Balkans

The identified key gaps and challenges and the contributory factor to understanding the existing context of building resilience to crises and disasters in the six economies of the Western Balkans Region are summarized as the following:

• The existing critical infrastructure frameworks in the six economies in the Western Balkans Region are predominantly *reactive*, focused on protection, rather than *proactive,* focused on prevention and mitigation and contributing to the overall resilience-building of the critical infrastructure.

• Low awareness of the importance of the critical infrastructure and the resilience-building process by the key policy- and decision-makers, professionals and practitioners.

• Even though all countries adopted or will adopt laws on critical infrastructure i.e. North Macedonia, the existing policy and normative framework are not finalized since necessary strategic documents, by-laws, rulebooks, SOPs and other documents create potential vulnerabilities in the different CI sectors. Also, the adopted legislation needs to be timely harmonized with the EU directives from this area.

• Enforcement of these CI-related policies and normative frameworks is still at a low rate and not all relevant institutional mechanisms are established.

• The status of critical infrastructure protection at all levels of government is inadequate due to weak, non-integrated, and non-systemic organization of sectors that may constitute critical infrastructure. Not all sectors are formally designated and approved by the relevant authorities. If not regulated accordingly, the involvement of multiple institutions leads to fragmented coordination and communication, which may hamper the efficient management

of critical infrastructure protection. Inadequate coordination and planning between various aspects of critical infrastructure systems.

• In all six economies, there are limited capacities and knowledge to develop and implement CI resilience-building-related policies and to mainstream the critical infrastructure across the development sectors, policies, programmes and plans. In this sense, integration with the cyber security area is still lagging behind the needs following the recent cyber attacks. „Integration is not sufficient to reflect the systemic nature of the risk and the interconnectivity and interdependence of the CI systems, which seek to better address the needs for inclusiveness and building resilience. The approach itself needs to be considered, mainly the infrastructure facilities and assets, rather than the services provided or resources allocated. Most of the sectors have "a silo approach" rather than an "all-hazard" approach or a "CI life-cycle" perspective."[33]

• National Platforms for Disaster Risk Reduction where established are not comprehensively included in the resilience-building measures and actions.

• The critical infrastructure sectors and sub-sectors are not comprehensively assessed against existing and emerging risks and threats, followed by the preparation of detailed operational plans.

• Monitoring systems for the operation and functioning of the critical infrastructure sectors and sub-sectors are still not in place in all of them.

• Still, there is a low rate of CI entities in the Western Balkans region that have prepared, regularly tested and update business continuity plans to ensure the timely, effective and efficient provision of services, predominantly because of a lack of relevant legislation, professional knowledge and technical expertise.

• Insufficient resources and expertise, varying from inadequate human resources, limited finances or availability of material and technical resources for operation, maintenance and protection.

• Lack of specialized technical expertise in public institutions for dealing with new and emerging risks and threats i.e. cyberattacks.

• Even though the private sector bears the biggest part of the disaster damages (on a global level there is an estimation that approx. 80% of the damages and losses are accounted to the private sector) and it operates the majority of CI systems, the roles, responsibilities and potentials for partnering and cooperating in the building of the

[33] Vasko Popovski. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP. 2022. p.32. [Online] Available at: https://tinyurl.com/3hm772n4

critical infrastructure resilience are not sufficiently recognized and utilized.

• Professional organizations and informal communication networks provided very strong support for prevention, risk management and emergencies. However, these organizations are not given legal positions, resources and scope for much more comprehensive roles.

• As presented below, there are many good practices and lessons learned in the region, but they are not evaluated, codified and transformed into workable solutions for building critical infrastructure resilience.

• Insufficient use and application of ICT innovative solutions for building the resilience of the critical infrastructure.

5. Good practices in building the resilience of the critical infrastructure in the Western Balkans

• ***Albania: Building the resilience of infrastructure through climate change adaptation*** – Climate change is projected to have a considerable impact on society and communities in the future. The temperature is expected to rise,[34] and precipitation will decrease, but its intensity would increase and the sea level will is expected to rise affecting the coastal communities. These projected impacts will pose additional stress to all development sectors and critical infrastructure. Therefore, Albania included the measures and actions for building the resilience of the infrastructure through the prism of climate change adaptation. The recently adopted National Adaptation Plan (2021) focuses on Governmental preparedness for a long process of climate change adaptation. It provides a framework for targeted mainstreaming and implementation of prioritized actions and it is a catalyst for meaningful participation, fostering partnerships and broader awareness raising. In particular, it refers to the following sub-sectors i.e. water supply (No. 7: Climate resilient irrigation, drainage and flood protection), agriculture sector (No.9 Adapted farm production), as well as the development of standards for resilient infrastructure i.e. incorporation of sea level rise into the new infrastructure planning or integration of the climate change scenarios into the water supply sector.

• ***Bosnia and Herzegovina: Energy-efficient Building Back Better*** - Following the May 2014 Floods, the country invested a lot in energy-efficient retrofitting of public buildings including a significant number of education, healthcare and public facilities. The usual recovery approach was integrated with energy efficiency practices allowing them to be institutionalized and co-financed in public facilities rehabilitation thereby enhancing the level of ownership and broadening the recovery process and intervention. The practice

[34] https://tinyurl.com/mtf59ydu

has shown numerous economic, environmental, utility system and disaster risk management benefits for the communities and local authorities enabling them to further invest in the resilience of the local critical infrastructure.

• ***Montenegro: Fostering public-private partnerships for disaster risk assessment*** – Montenegro encourages and supports public-private partnerships in the development and management of critical infrastructure, which can lead to improved resilience-building and resource mobilization activities. This led to the establishment of a multi-sector working group for the development of the Disaster Risk Assessment of the country. This significant undertaking involved various professionals and experts from government institutions, "public enterprises, academia, NGOs, and the private sector. The Ministry of Interior - Rescue and Protection Directorate served as the main coordination authority, involving several state authorities and observing sectoral competencies. Consequently, the Disaster Risk Assessment of Montenegro identifies nine types of risks, 51 individual risk scenarios, and eight multi-risk scenarios, and includes 53 risk maps. This document was recognized as an important input for the process of National Adaptation to Climate Change Plan preparation in Montenegro, attaining Paris Agreement objectives, Sustainable Development Goals achievements etc."[35]

• ***North Macedonia: Enhanced risk understanding by inventorization of critical infrastructure*** – Most of the country's critical infrastructure is inventoried by the Crisis Management Centre and included in the national and 81 municipal risk and hazard assessments as part of the analysis of the exposure and vulnerability of the risk elements. This inventorization of the elements of risk (infrastructure) is part of the E-Assessment Platform and contains information on the following assets and facilities i.e. construction objects (hydro-construction objects i.e. dams and water supply facilities, traffic objects i.e. railways with normal gauge, railway bridges, overpasses and underpasses, highways, regional roads, local roads, tunnels and galleries and airport runways, electric power and other transport objects i.e. electric power line and networks, power substations and oil and gas pipelines. Within the category of economic buildings and objects following ones are identified: industrial facilities, motels and recreation centres, halls and hangars, silages, freezers, reservoirs and tanks, warehouses

[35] Ministry of Interior – Protection and Rescue Directorate. Voluntary Review and Report of Montenegro. Podgorica, September 2022. p.10. [Online] Avialble at: https://sendaiframework-mtr.undrr.org/media/84438/download

for products/materials, buildings for rail traffic, buildings for water and air traffic, buildings for road traffic, buildings for trade, hotels and temporary facilities. Non-economic buildings refer to school buildings, buildings for art and culture, social and health protection, sport and recreation, shelters and other facilities. Treasuries are considered to be cultural treasures and objects. Each type/object of the critical infrastructure has more than 20 attributes relevant to its vulnerability and usage within the risk reduction efforts.

• ***Western Balkans Region: Strengthening cybersecurity and building resilience*** – Following the unprecedented series of cyber attacks, the WB economies have taken steps to enhance the cybersecurity of critical infrastructure through the prism of two actions. Firstly, through the establishment of Computer Incident Response Teams to be engaged in handling the information security incidents in the countries. Additionally, France, Montenegro and Slovenia signed a Letter of Intent in November 2022 to establish a Centre for Cybersecurity Capacity Building in the Western Balkans with a headquarter in Podgorica. The centre's training activities, which will be fully based on EU standards, will cover cybercrime, cybersecurity and digital diplomacy. In addition, this facility will strengthen the operational and institutional response capabilities of governments throughout the Western Balkans to deal with cyber threats and attacks.

6. A way forward to build the resilience of critical infrastructure in the Western Balkans

Based on the above-identified gaps and challenges and findings during the desk review part of the preparation of this paper, a set of general recommendations is formulated to serve as a departing point for both regional and national interventions for building the resilience of critical infrastructure in the Western Balkan Region. These forward-looking recommendations focus on creating an enabling environment for re-shifting the approach to critical infrastructure, from protection to building its resilience to crises and disasters. Accordingly, they are summarized as follows:

• The complexity of critical infrastructure requires enhancing the policy and normative frameworks enabling resilience-building of the critical infrastructure by the adoption of new or modification of the existing policies and legislative solutions. One of the priorities in this sense is the consequent transposition of the recent and other EU directives e.g. Directive on the Resilience of Critical Entities and NIS² Directive to update the national framework and to harmonize the legislation in this area.

• Adapting the institutional architecture by the adoption of critical infrastructure protection systems i.e. identifying the European Critical Infrastructure, designating coordination entities, systematization of their roles and responsibilities, designing and implementing awareness-raising activities, as well as the establishment of national critical infrastructure centres that would be responsible for operative, consulting, analytic and inspection aspects.

• Sensitization of key stakeholders on the critical infrastructure resilience and crisis and disaster risk management (NDMAs and related stakeholders on the critical infrastructure aspects vs. operators/owners on resilience and contemporary crisis and disaster risk management).

• Ensuring cross-sectoral cooperation and coordination at every level and amongst all stakeholders ensuring the needs of the most vulnerable ones are reflected and systematically integrated into the critical infrastructure framework while leaving no one behind, especially in the provision of critical infrastructure services domain.

• Implementation of research studies on the resilience aspects of the critical infrastructure systems and understanding of their interdependency and complexity alongside the systemic nature of risks, including the resilience of the critical infrastructure in uncertain times based on non-linear risk assessments.

• Multi-risk, multi-hazard, multi-stakeholder assessment of exposure and vulnerability of the critical infrastructure systems considering both the disaster and climate risks should be done in coordination with the owner and operators needs to be comprehensively incorporated in the existing and new operational planning documents ensuring the resilience of the societies and communities.

• Risk modelling, scenario planning and training exercises are vital for testing the resilience of the critical infrastructure sectors and the capacities and readiness of the operators for better preparedness and response to existing and future risks and this approach needs to be embedded into the NDMAs and operators' regular work and competencies.

• Development of contingency planning and business continuity of the critical infrastructure sectors ensuring their integration with adequate national and local planning documents.

• Application of the Guidance Notes on building critical infrastructure resilience in Europe and Central Asia as practical tools to support the authorities and practitioners in the WB countries in designing relevant resilience-building policies and implementing adequate actions in partnership with other entities, owners and/or operators before, during and after crises and disasters.

• Designing and implementing projects aimed at building the national, cross-border and regional critical infrastructure and boosting regional cooperation and coordination in this sense.

• The private sector needs to be a driver of transformational change in the resilience building of the critical infrastructure and needs to be included in all related processes and activities e.g. policy design, normative and institutional frameworks establishment, standardization and implementation of actions and measures for resilience, transfer of

knowledge and expertise, capacity development, etc.

• Investments in the resilience building of the critical infrastructure need to be done in partnership with the private sector, both the owners and the operators of the existing systems, as well as external investors considering the economic attractiveness of the infrastructure resilience utilizing the existing financial mechanisms and new ways for financing resilience.

• Utilization of the public-private partnerships as a modus operandi for resilience building of the critical infrastructure combining the public sector knowledge and efforts and private sector expertise and resources.

• Capacities strengthen the key stakeholders and empower other DRR actors to contribute to the resilience-building of the critical infrastructure alongside enhancing their knowledge and professional and technical expertise i.e. investing in training and capacity development of infrastructure operators and emergency responders.

• Raising the awareness of the involved key stakeholders and the general public on the importance of critical infrastructure and building their resilience to crises and disasters.

• NDMAs are in the position to manage the resilience building of the critical infrastructure and therefore a mechanism of regular monitoring and evaluation and review of actions can be a practical and beneficial tool for consequent actions.

• Leverage the power of partnerships for resilience building of the critical infrastructure including the emphasized role of the National DRR Platforms that can contribute through a palette of activities i.e. initiating thematic discussions on the resilience-building of the critical infrastructure, increasing the awareness of the key stakeholders, participating in research and development activities, supporting the strategic and normative policy creation, contributing to enhanced public awareness, knowledge, information and best-practices sharing, etc.

• Identifying the possibilities for further decentralization of critical infrastructure sectors enabling the local level authorities better governance of existing, anticipated and new risks and futures.

• Recent experiences showed that critical infrastructure systems are vulnerable to cyberattacks and therefore the national authorities, NDMAs and the systems owners/ operators need to ensure the implementation of sound ICT information security policies and actions regularly updated to the new risks and threats ensuring business

continuity of their operation and provision of services.

• Designing and applying ICT innovative solutions for supporting resilience-building efforts. In this sense, AI, big data, and high-performance computing can provide significant support, alongside other innovative methodologies and tools. Leveraging their application creates an opportunity for better preparedness and response to the increased types and many cyber-attacks on the viral critical infrastructure.

7. Conclusions

This Policy Paper provided a detailed overview of the overall critical infrastructure framework and national contexts in the six economies from the Western Balkans and formulation of forward-looking recommendations aimed at supporting the efforts for building the resilience of the critical infrastructure to crises and disasters. Furthermore, it aims to advocate for initiating transformational change in understanding and applying the resilience-building approach throughout the critical infrastructure domains.

Critical infrastructure resilience is understood as *the ability of these systems to absorb, adapt to and/or rapidly recover from a potentially disruptive event*. The most effective way in this sense is to shift the paradigm of critical infrastructure from risk to resilience, from protection to building resilience by designing and applying preventive measures and actions. The six economies in the Western Balkans embarked on the journey to build the resilience of vital infrastructure systems on their territories following the EU lead on this matter and following the global mechanisms and best practices. The review has shown that the countries are on different levels of development and to achieve the goal of resilience it is needed to continue with the policy, normative and institutional development to ensure harmonization and application of not only the latest regulations and standards but also their mainstreaming across the sectors, especially the security one.

It is evident that the countries are lacking the necessary professional and technical expertise, and sufficient cooperation with the private sector, research and development entities and academia, therefore it is necessary to design appropriate education and training curricula, to foster partnerships with the private sector and other actors utilizing and sharing the resources, knowledge and expertise. Building the resilience of the critical infrastructure requires a "whole-of-government" and "all-of-society" approach and during the designing and implementing policies, measures and actions these processes need to be inclusive and participatory ensuring that the provision of related services will leave no one behind.

Even though the national contexts and the countries' crisis and disaster risk management systems are various, the regional approach in this resilience-building endeavour is the *modus operandi* for intensifying these activities and contributing to the safer, more secure and resilient Western Balkans.

Bibliography

Denis Cenusa. EU Eastern Enlargement: Preparing for Current and Future Threats Through Inclusive Crisis Management and Resilient Critical Infrastructure (Web-article). SCEEUS Guest Platform for Eastern Europe Policy No. 21. 18 January 2023.

Dr. Simone Sandholz. Five things you need to know about critical infrastructures (Blog). UNU-EHS. 2017.

Craglia, M. et al., 2020, Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis. JRC Science for Policy Report, JRC121305. Geneva Centre for Security Sector Governance. National Cybersecurity Strategies in Western Balkan Economies. 2021.

Luca Galbusera, Monica Cardarilli, Georgios Giannopoulos. "The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures". Safety Science, Volume 139. 2021.

Nermin Oruc, Saima Raza and Danica Santic. Analytical Report: The Western Balkan Migration Route (2015-2019). Prague Process Secretariat. March 2020.

Santiago Lema-Burgos. Disaster Risk to Critical Infrastructure: Understanding critical infrastructure in the ECIS region. UNDP. 2019.

Sulmet iraniane, Artan Hoxha: Hakerat kanë marrë çdo gjë, edhe sistemin banker, Gazeta Tema, 11 Tetor 2022.

The World Bank. Western Balkans Face New Economic Headwinds Despite Strong Post-Pandemic Recovery (Press-release). 2022.

UCP Knowledge Network. Disruption to Critical Infrastructure (Web-article). 27 June 2022.

UNDRR—Regional Office for Europe & Central Asia. Sendai Framework Monitoring in Europe and Central Asia: A Regional Snapshot. December 2020.

UNEP. Regional Strategy For Climate-resilient Road Infrastructure. ADC/ UNEP. 2022.

Vasko Popovski. Assessment Study of the Role of NDMAs in COVID 19 Crisis Response and Impact of Covid on NDMAs Operations. UNDP/UNDRR. 2020.

Vasko Popovski. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP. 2022.

V.S. Nageswara Rao Kadiyala, Ripon Patgiri, Chapter Seventeen - An investigation on socio-cyber crime graph, Editor(s): Ripon Patgiri, Ganesh Chandra Deka, Anupam Biswas, Advances in Computers, Elsevier, Volume 128, 2023, Pages 423-443

Information about the International Visegrad Fund

The Visegrad Fund is an international donor organization, established in 2000 by the governments of the Visegrad Group countries—Czechia, Hungary, Poland and Slovakia to promote regional cooperation in the Visegrad region (V4) as well as between the V4 region and other countries, especially in the Western Balkans and Eastern Partnership regions. The Fund does so by awarding €8 million through grants, scholarships and artist residencies provided annually by equal contributions of all the V4 countries. Other donor countries (Canada, Germany, the Netherlands, South Korea, Sweden, Switzerland, the United States) have provided another €10 million through various grant schemes run by the Fund since 2012.

Address:
Hviezdoslavovo námestie
9 811 02 Bratislava Slovakia

https://www.visegradfund.org/

Information about THINK BALKANS

The 'Enhancing Think Balkans – knowledge hub for Western Balkans EU integration and regional cooperation" project is financially supported by the International Visegrad Fund and builds upon the previously established cooperation between the members of the Southeast European Think Net Network (SEE Think Net) and Think Visegrad as part of the 'Regional cooperation in the Western Balkans: The Berlin Process and Visegrad Group in comparison project' and the project "Cooperation Instrument for the Western Balkans Think Tanks – THINK BALKANS" supported by the International Visegrad Fund.

Following the successful past cooperation, the **Institute for Democracy "Societas Civilis" – Skopje (IDSCS)** will remain project coordinator, which, in collaboration with the **European Movement in Serbia (EMinS)**, **Balkan Research Institute** from Kosovo*, **Politikon Network** from Montenegro, **Albanian Institute for International Studies (AIIS)** from Albania, **Humanity in Action** from Bosnia and Herzegovina, **Centre for Eastern Studies (OSW)** from Poland, **Institute for Foreign Affairs and Trade (IFAT)** from Hungary, the **Research Centre of the Slovak Foreign Policy Association (RC SFPA)** from Slovakia, and **EUROPEUM Institute for European Policy (EUROPEUM)** from the Czech Republic, will work in achieving the project's goals.

The project duration is 12 months, that is, from October 2022 to October 2023.

Based on the lessons learned, this project proposal aims to promote active participation in policy-making and foster democratic debate based on relevant data and information by further: 1) promoting cooperation among think tanks, CSOs and experts in the WB as a successful regional model; 2) strengthening the cooperation with the WB MFAs through the establish network of contact point and include their opinions and ideas in specifying the details of the topics chosen to be analyzed through this project; 3) providing V4 expertise on security, resilience and EU enlargement in general in light of the Russian invasion on Ukraine and the expressed interest of the Associate trio countries to join the EU; 4) using the potential with the establishment of Think Balkans to strengthening people-to-people links between the WB and V4; 5) cultivating interregional cooperation between V4 and WB6 on issues of common strategic interest.

About the authors:

Vasko Popovski, M.A., is an independent, researcher, consultant and practitioner with many years of experience in the areas of crisis management, disaster risk management, urban resilience and innovations for resilience. His expertise in professional areas of operation extends to the countries of the region of Europe and Central and South-East Asia and beyond. He has a law degree, completed postgraduate studies in political science and is a doctoral candidate in security sciences. During 2018/2019, as a Fulbright Fellow and guest researcher, he was part of the team of the Disaster Research Center at the University of Delaware, USA, where he realized part of his PhD research on the topic of resilience and the model of a resilient society and participated in the realization of the teaching curriculum. In addition to this, the area of building the resilience of critical infrastructure is the newest area of professional interest and in that sense, in 2022 he authored the Guidance notes on building critical infrastructure resilience in Europe and Central Asia commissioned by UNDP Europe and Central Asia.

Ledion Krisafi, is a Senior Researcher at the Albanian Institute for International Studies (AIIS) since 2016. His main areas of interest are: Balkan history, geopolitics and security. He has published several studies and articles in these topics. Also, he has published a book about relations between Albania and Yugoslavia in the years 1945-1948. He has a Ph.D in International Relations and Political Sciences from the European University of Tirana.

Ana Nenezić (PhD candidate in International Relations at the Faculty of Political Sciences in Podgorica, University of Montenegro) is an Executive Director of the Center for Monitoring and Research (CeMI). Ana specializes in strategic communication, political campaigns, and the impact of digital technologies and traditional media on voters' attitudes. Ana is the author and co-author of numerous publication, analyses and articles focusing on various aspects of democracy, European integration, elections, and freedom of expression.

Sead Turčalo is an associate professor and Dean of the Faculty of Political Sciences at the University of Sarajevo. In the first and second cycles of the Department of Security and Peace Studies and Political Science, he teaches the courses Geopolitics, International Security, and Energy Security and Conflict Management in International Relations. In the interdisciplinary doctoral study

of the Faculty of Political Sciences of the University of Sarajevo, and in the doctoral program of Global Studies of the Center for Interdisciplinary Studies UNSA, he is a co-lecturer in the Geopolitical Studies of the Contemporary World course.

Donika Emini (PhD candidate in Politics and International Relations at the University of Westminster, London) is leading the CiviKos Platform, a secretariat gathering 270 CSOs in Kosovo* and Balkan Research Institute. Her field of expertise includes regional cooperation, dialogue between Kosovo* and Serbia, security cooperation between Western Balkans and the EU (CSDP). She has been actively working in the Eastern Partnership Countries on cybersecurity as part of the EU funded projects.

Aleksandar Kovacevic started his professional career with the Federal Productivity Institute of Former Yugoslavia in 1986. Over 20 years he provides strategic advice, complex energy efficiency solutions and emergency situation assistance to major institutional, financial and private clients including assistance to UN OCHA to coordinate rapid reconstruction of Serbia energy infrastructure after 1999 war. He was affiliated to PlanEcon before 1992, project manager for Tagarnrog Development project in Russia (1992-1998) and contributor to the Black Sea and Central Asia panel at the Harriman Institute, Columbia University.

Link

This publication is available at:
https://idscs.org.mk/en/2023/05/02/crisis-prevention-and-critical-infrastructure-in-western-balkans/

This project No. 22220222 was made possible through Visegrad+ Grant from the International Visegrad Fund.

IDSCS

AIIS ALBANIAN INSTITUTE FOR INTERNATIONAL STUDIES

HUMANITY IN ACTION BOSNA I HERCEGOVINA

BALKAN RESEARCH INSTITUTE

POLITIKON

European Movement Serbia

EUROPEUM INSTITUT PRO EVROPSKOU POLITIKU INSTITUTE FOR EUROPEAN POLICY

INSTITUTE FOR FOREIGN AFFAIRS AND TRADE

SFPA Slovak Foreign Policy Association

OSW