KCSS
Kosovar Centre for Security Studies

EMERGING THREATS PROGRAMME

WHAT CAN KOSOVO LEARN FROM THE BALTIC STATES' APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION?

Author: Donika Elshani

November 2023

Supported by: SMART Balkans
Civil Society for Shared Society in the Western Balkans

EMERGING THREATS PROGRAMME

Author: Donika Elshani

About the Emerging Threats Programme

The Emerging Threats Programme has been designed as a response to evolving domestic, regional, and international security threats. Its primary aim is to consolidate and provide a better understanding of emerging threats that consistently move away from traditional conceptualizations of security challenges. Given the extent of evolving threats related to cybersecurity and disinformation, this programme seeks to build upon internal organizational capacities to provide evidence-based expertise to operationalize institutional responses to these challenges. Evidence-based research in relation to the Emerging Threats Programme focuses on: critical infrastructure, cybersecurity, disinformation and hybrid security challenges. While needs assessment(s), monitoring and research remain fundamental actions to be developed in the programme, KCSS aims to utilize expertise generated to directly enhance the capacities of executive institutions and agencies to respond effectively to cybersecurity challenges and disinformation. The programme will be developed through:

- State of the art evidence-based research related to emerging threats such as cybersecurity, critical infrastructure protection, hybrid threats and disinformation;
- Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity, critical infrastructure protection, hybrid threats and disinformation in Kosovo;
- Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity.

For more information, contact us at: EmergingThreats@qkss.org

This policy brief is published in the framework of the SMART Balkans project, implemented jointly by the Center for Civil Society Promotion, the Institute for Democracy and Mediation (IDM) and the Center for Research and Policy Making (CRPM), with the support of the Norwegian Ministry of Foreign Affairs.

SMART Balkans
Civil Society for Shared Society in the Western Balkans

WHAT CAN KOSOVO LEARN FROM THE BALTIC STATES' APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION?

November 2023

Table of contents

Executive summary

Critical infrastructure, encompassing vital systems and assets crucial for societal functioning, faces a diverse range of threats, from climate change-induced natural disasters to human-made errors and disasters. The Western Balkans, including Kosovo, are not immune to these challenges. In the context of Kosovo, ethno-political tensions, severe floods, and cyberattacks are just a few examples of the threats that pose significant risks to its critical infrastructure. In April 2019, Kosovo adopted the Law on Critical Infrastructure, becoming the first country in the region to do so in line with the EU directives. Nevertheless, the implementation of the law has been lacking, leaving much room for improvement and further action.

The purpose of this policy brief is to support the efforts of public institutions, with a particular focus on the Ministry of Internal Affairs (hereafter MIA), in designing and implementing an effective and comprehensive critical infrastructure system in Kosovo. The brief aims to provide an overview of best practice examples from the Baltic states, which have come to be recognized as leaders in the fields of cyber security and critical infrastructure resilience. The Baltic states, which include Estonia, Latvia, and Lithuania, provide a good basis of comparison for Kosovo in this field, not least because of their similar historical challenges, geographical proximity, and similar demographic profile. Unlike the Baltic states, Kosovo is at the initial stages of establishing its critical infrastructure protection framework. Although the sector is far from being fully operational, this stage offers a valuable opportunity for the involved institutional actors in Kosovo to learn from countries like the Baltic states.

Kosovo can learn several important lessons from the experiences of Estonia, Latvia, and Lithuania in critical infrastructure protection by implementing these lessons and considering the specific challenges and needs of its own infrastructure and security landscape.

- **Foster a Security Culture:**

  Building a strong security culture among all institutional stakeholders is vital. Increasing awareness about the importance of securing critical infrastructure and cooperating on resilience is essential.

- **Assign a Leading Entity:**

  Clarify which institutional entity assumes a leading role in the critical infrastructure sector (i.e., Division in MIA). Consider whether the Government Office should take a more central coordinating role, as this can facilitate coordination among sectoral ministries. Also, consider is the level of Division provides sufficient authority for this unit to effectively coordinate implementation of the law. Perhaps promote the division to a status of a department or agency.

- **Streamline Legal and Organizational Structure:**

  Establish a coherent and well-designed system from the beginning to avoid complications in the future. Streamlining legal norms and the organizational structure can enhance efficiency. Kosovo can do this in the process of finalizing the secondary legislation for implementation of Law No. 06/L-014 on Critical Infrastructure.

- **Focus on Protecting Services:**

  Consider a shift towards protecting critical services rather than individual objects. Prioritizing service continuity and recognizing the inter-connected nature of critical infrastructures is essential.

- **Allocate Resources for Civil Preparedness:**

  Develop tools and resources to strengthen civil preparedness in the event of critical infrastructure disruptions. Initiatives like preparedness applications and crisis response guidelines can be valuable.

Introduction

Critical infrastructure is a concept that refers to the physical and virtual systems that are vital for ensuring the proper functioning of essential services in a country. Critical infrastructure gained renewed attention in the aftermath of the 9/11 terrorist attacks against the United States of America, which served as a significant catalyst for recognizing the vulnerabilities of essential systems and the need for their protection. Depending on the country, critical infrastructure may include sectors such as energy, transportation, telecommunications, healthcare, water, and food supply. As societies became increasingly interconnected and reliant on digital technologies, the landscape of critical infrastructure protection has expanded to include cyber-related threats or cyber infrastructure. Information and communication technologies have come to play a crucial role in connecting critical infrastructure systems worldwide. Major critical infrastructure systems often rely on some level of software-based control systems for their operation. The risks and vulnerabilities that come with the interconnected nature of these systems pose a significant challenge. Attacks on one sector can have cascading effects on other sectors, thereby resulting in major societal disruptions that span various functions and public services.

Russia's invasion of Ukraine and the geopolitical shifts it triggered, have caused significant disruptions in critical infrastructure systems across Europe, that affected various parts of the world. Western sanctions imposed on Russia accelerated a global energy and food crisis, leading to a breakdown in oil and gas supply chains, on the one hand, while triggering a decline in supply of staple food and a rise in food prices worldwide, on the other.[1]

The effects of the Russian invasion of Ukraine were felt in the Western Balkans as well, raising concerns about Russia's destabilizing influence in the region through its allies in Serbia and in Bosnia and Herzegovina (Republika Srpska). Russia has a track record of implementing disinformation campaign and exercising malign influence in the Western Balkans in order to counter integration of the region in the European Union (EU) and NATO.[2] A series of cyber-attacks targeting the digital state infrastructures of several countries in the region, including Montenegro and Albania, have raised suspicions about the involvement of Russian and Iranian state security bodies in these incidents.[3]

The vulnerability of critical infrastructure in the Western Balkans has been exacerbated by climate-related disasters. For instance, Albania was hit by a devastating 6.4 magnitude earthquake in 2019, leaving 51 people dead and injuring thousands. The earthquake caused deaths and widespread damage, critical state infrastructure, including social infrastructure such as schools and hospitals.[4] Kosovo, like many other countries in the region, experiences recurring floods caused by heavy rains. In January 2023 Kosovo was hit by severe floods which resulted in water shortages and reductions in the supply of drinking water for several towns in the western and northern regions of Kosovo. The floods also caused significant traffic issues, landslides, and flooding of agricultural land in several areas.[5]

Against the backdrop of these events, it is vital for Kosovo to invest and improve the protection capabilities of its critical infrastructure systems. In April 2019, Kosovo adopted the Law on Critical Infrastructure, becoming the first country in the region to do so in line with the EU directives.[6]

The implementation of the law, however, has not been satisfactory and there remains a lot to be done. For instance, the law foresees the establishment of the Division for Critical Infrastructure within the Ministry of Internal Affairs (MIA), which is to serve as the central mechanism responsible for overseeing the implementation of the law, including crucial elements such as the drafting of bylaws on the identification and designation of critical infrastructure sectors and the establishment of public-private partnerships, among others. While the Division has been set up, it has yet to be operationalized.[7]

As the 'Serbian threat' becomes increasingly prominent in Kosovo, especially following the recent terrorist attacks against Kosovo Police by Serb militants on September 24, 2023, in the village of Banjska, it is important that Kosovo takes a more proactive approach towards building resilience and security of critical infrastructures, including critical information infrastructure.[8]

The remainder of the policy brief is structured as follows: the first section provides an overview of the regulatory framework of critical infrastructure protection in Kosovo. The subsequent three sections discuss critical infrastructure strategies and practices in the three Baltic States – Estonia, Latvia and Lithuania, before delving into lessons and take away points for Kosovo based on the experiences of the Baltic States.

Policy framework of critical infrastructure protection in Kosovo

The process of legal regulation of the critical infrastructure sector in Kosovo began in 2014, when the MIA drafted the Concept Document for the Identification and Protection of Critical Infrastructure, which resulted in the approval of the Law on Critical Infrastructure in 2018. The law combined the American and Croatian experience and legal concepts of regulating the critical infrastructure sector, as well as the EU approach through Directive 2008/114/EC on the identification and designation of European critical infrastructures.[9] The law was published in the Official Gazette of the Republic of Kosovo in May 2018, and subsequently entered into force in April 2019.

The Law on Critical Infrastructure consists of five chapters and 23 articles in total, covering issues such as the regulation of national critical infrastructure, the operator security plan and security coordinators, European critical infrastructure and monitoring, supervision, and evaluation.[10] One of the highlights of this law is the establishment of the institutional mechanism within the MIA to oversee the implementation of the law. In accordance with the law, the establishment of the Division for Critical Infrastructure within the MIA was included in the Regulation on the Internal Organization and Systematization of Positions in the MIA, adopted in January 2021. Based on the regulation, the division operated in the framework of the Department for Public Safety and among others, it is responsible for proposing, drafting, and ensuring the implementation of the legal framework, leading critical infrastructure projects and serving as a point of contact for all issues relating to the sector. An updated version of the MIA internal regulation also included plans for the staffing of the division with four officials.[11]

Based on Article 4, the Division for Critical Infrastructure, as part of the institutional structure of the MIA, was to be established and fully functional within three months after entry into force of the law, which was in 2019. However, it has been four years since then and the division is still not operational. This constitutes a direct violation of the legal obligations of the Kosovo government. Furthermore, this has put the implementation process of the law itself at a standstill as the entire legal framework largely depends on the operationalization and effective functioning of this division. For instance, the law assigns the division with the task of initiating the process of identifying national critical infrastructure in the country, a process that was to be finalized within six months after entry into force of the law.

The lack of a list of national critical infrastructure hinders the subsequent process, which is that of designating these objects or systems. Furthermore, without a division that is to act as a liaison between various stakeholders, no public-private partnerships can be established effectively. The involvement of the private sector in critical infrastructure protection is crucial as most of the critical infrastructures in the country are owned or operated by private entities. Altogether, the lack of implementation of the Law on Critical Infrastructure poses serious concerns not only to the security of certain critical infrastructure objects or systems, but to national security as a whole.

This is an opportune moment for Kosovo to look towards other countries with sophisticated critical infrastructure management systems such as the Baltic States. The following section provides a general overview of strategies and practices in Estonia, Latvia and Lithuania.

A glimpse at critical infrastructure strategies and practices in the Baltic States

The Baltic states, comprising Estonia, Latvia, and Lithuania, have emerged as pioneers in the field of critical infrastructure protection. The evolution of the system for critical infrastructure protection in these countries has been marked by a series of internal and external threats that have shaped their strategies and practices over a 30-year period. The process can be traced back to the 1990s when the three Baltic states declared independence from the Soviet Union. Inheritance of the Soviet approach, which was largely focused on the protection of critical objects from external opponents, shaped the early stages of regulating the sector in these countries, most notably in Latvia. The 9/11 terrorist attacks in 2001 shifted the global security agenda, leaving its footprint in the Baltic region as well.[12] This not only impacted the evolution of the critical infrastructure protection in these countries towards a heightened focus on counter-terrorism activities, but also underscored the importance of addressing the broader problem of protecting vital functions in a society.

Rapid advancements in technology and the integration of digital technologies have transformed critical infrastructure systems, making them more inter-connected and efficient while also expanding the scope and complexity of potential threats. It was during this period that the Baltic states experienced some of the most prominent internal attacks, including the data leak from Latvia's tax authority in 2010[13] and the 2007 cyber-attacks targeting the websites of Estonian governmental, political, and financial entities.[14]

Another pivotal factor has been the role of the international community, most notably the EU and NATO. The introduction of EU legislation on European critical infrastructure fostered greater alignment of the approaches of the Baltic states. In 2010, all three Baltic states transposed the Directive on European critical infrastructure into their national legislation. This directive establishes the conditions for identifying and protecting critical infrastructure at the European level.[15]

Lastly, but surely not the least important is the Russian threat to these states, particularly in the aftermath of the invasion of Ukraine. The war in Ukraine has demonstrated Russia's intent and capabilities to project military power in the Baltic region, including through information warfare. Responding to this threat, the three Baltic states have significantly boosted defense spending since the onset of the war.[16]

When it comes to the normative frameworks and the organizational structures of the critical infrastructure system, the three Baltic states have their share of similarities and differences.

The case of Estonia

In Estonia there are two approaches to addressing critical infrastructure protection: first, under the concept of 'continuity of vital services' as part of crisis management within the broader national defense framework and second, through the physical protection of national defense objects.[17] The continuity of vital services is regulated by the Emergency Act, the foremost legal act that governs Estonia's response to emergencies, whereas the protection of national defense objects is regulated by the National Defense Act.[18] The concept of 'continuity of vital services' can be viewed as analogous to the concept of critical infrastructure protection. Pursuant to Article 34 of the Emergency Act, the continuity of a vital service is defined as "the capability of consistent functioning of the organizer of the vital service and the ability to restore the consistent functioning after an interruption".[19] On the other hand, the National Defense Act defines a national defense object as any land, building, or device that, if targeted, can pose a threat to national security, public order, the functioning of the state, military organization, internal security, vital services, or cultural heritage.[20]

There are a total of 14 vital services defined in the Emergency Act, whereas the list of national defense objects is unknown since it is classified information. The Government Office recently replaced the Ministry of Interior as the lead agency in crisis management, while the Internal Security Service leads the process of protecting national defense objects. Some of the responsibilities of the Government Office in this respect are the development and execution of national crisis management policy and provision of counseling and guidance to other stakeholders involved in the sector.[21] Importantly, however, is that the Government Office is not the sole entity that keeps the system running. The Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, the Bank of Estonia, and the authorities of localities with over 10,000 residents are also involved in ensuring the continuity of vital services. These entities have the responsibility of organizing and maintaining the continuity of services within their respective sectors. This includes ensuring the uninterrupted supply of electricity and natural gas, the functionality of national and local roads, phone services, emergency care, payment services, and the availability of water supply, among other essential services.

Another important group of stakeholders which are providers of vital services are both private and state-owned companies. There are specific legal acts that set out the criteria for vital service providers, and include, for instance, the Electricity Market Act, the Electronic Communications Act, the Natural Gas Act, the Public Water Supply and Sewerage Act, etc. The number of providers and the list of services they protect are not made public.

The case of Lithuania

The protection of critical infrastructure in Lithuania is based on two regulatory ecosystems. The first one is founded on the Law on the Protection of Objects of Importance to National Security, which establishes a defined list of enterprises, facilities, property, and territory deemed crucial for national security. These objects span various sectors, including energy, transport, IT and communications, finance, and military equipment. Importantly, the law imposes obligations and restrictions on activities, transactions, investments, and transfers of ownership to safeguard Lithuania's national security interests by mitigating any risk factors that could potentially pose a threat.[22] The primary focus of the Law is to regulate business transactions, investments, and other commercial activities in order to safeguard national security interests as outlined in the National Security Strategy.[23] The second regulatory pillar evolved in response to discussions surrounding potential privatization agreements and attempts of Russian companies to gain shares in enterprises in the strategic sectors in Lithuania.

The Commission for coordination of the protection of objects important to ensuring national security, formed by the Government of Lithuania, is the entity in charge of oversight and management of this system. Specifically, the Commission holds authority in making crucial decisions pertaining to investments, share transfers, equipment acquisitions, ICT systems, and other transactions involving enterprises deemed significant for national security.[24] Decisions are made on the basis of the origin of investors, on the one hand, and risk assessment, such as cyber risks, energy and economic dependency, on the other. The Vice Chancellor of the Government is the chair of the Commission, which is comprised by representatives from various ministries, as well as the Bank of Lithuania, the Prosecutor's Office, the State Security Department, to name a few.

The second ecosystem – that of critical information infrastructure – was established in 2016 and later revised in 2018, and it specifically addresses objects vital to services of special importance. This system was established through a Government Resolution which lists 14 sectors of critical infrastructure. The system is based on a top-down approach and consists of several steps. First, the Government of Lithuania designates particular services and sectors as critical infrastructure. Secondly, each sectoral ministry or other state entity responsible for overseeing a specific sector carries out an assessment to determine which objects meet the criteria for inclusion in this category. This assessment is undertaken jointly with the operator or owner of the selected object using a specialized questionnaire. When an object reaches a predetermined threshold score, it indicates that any disruption to the service provided by such objects would have negative impacts and it should thus be categorized as a critical infrastructure object.

As part of the systemic changes made in 2018, the coordinating role for this system was assigned to the National Cyber Security Center, established under the Ministry of Defense, which, among others, is responsible for ensuring quality control, providing methodological guidance, and serving as a central hub for managing cyber incidents. The Ministry of Defense also chairs the Cyber Security Council, a platform that

brings together stakeholders from the public and private sector, academia, the media, and other relevant entities, to monitor and discuss cyber security issues and public-private initiatives.[25]

The case of Latvia

In the case of Latvia, the critical infrastructure framework is divided into four strands: the national critical infrastructure, European critical infrastructure, essential services, and critical financial services. National-level critical infrastructure refers to objects, systems, or their components, as well as services within the territory of Latvia, that are essential for the execution of important public functions and the protection of human health, security, economy, and social well-being, disruption of which would have a significant impact on the fulfillment of public functions.

The European critical infrastructure consists of objects and systems in the energy and transport sectors, which, if destroyed or impeded, would have an impact on at least two member states of the European Union. Essential services are services that are dependent on network and operation systems across various sectors, such as water supply, internet, transport, and health, which are susceptible to cyber security incidents. Critical financial services are the latest addition to this list and include payment services provided by credit institutions.[26]

The foremost legal act that regulates critical infrastructure in Latvia is the National Security Law. This law provides the basis for the process of identifying national and European critical infrastructure, planning and implementation processes as well as operational continuity of critical infrastructure.[27]

When it comes to the institutional actors involved in national and European-level critical infrastructure, the Cabinet of Ministers, a collective body, approves the list of critical infrastructure, based on the proposal put forth by the Ministry of Interior. The latter is the main institutional entity driving policy-level debates, with the increasing involvement of the Ministry of Defense as well. At an operational level, state security institutions such as the State Security Service, the Defense Intelligence and Security Service, and the Constitution Protection Bureau, play a key role. These institutions are aided by the Latvian Computer Emergency Response Team (CERT.lv), which provides support and assistance with regards to information technology critical infrastructure. CERT.lv, in collaboration with the Digital Security Supervisory Committee, oversees the essential services in Latvia, while the responsibility for supervising the critical financial services lies with the Financial and Capital Market Commission and the Bank of Latvia.[28]

What can Kosovo learn from the Baltic states' approach to critical infrastructure protection?

Building a system for protection of critical infrastructure is a process which requires capacities and time, as the case of the Baltic states shows. These systems are a product of continuously adapting to an ever-changing internal and external threat landscape, years of continuous work, but most importantly, an ongoing evaluation process of what works within these systems and what doesn't.

Contrary to the Baltic states, Kosovo is still in the early stages of setting up its critical infrastructure protection framework. While the country still has a long way to go before the sector is fully functional, this juncture provides a good opportunity for the institutional actors involved in the sector to look to other countries and draw some valuable insights from these countries' experiences in building an effective critical infrastructure protection system.

Arguably, one of the strongest pillars of the critical infrastructure protection framework in the Baltic states is the **security culture** that permeates the entire ecosystem. While the responsibility for critical infrastructure protection in each respective Baltic state is shared among various stakeholders, the advantage of the systems is that there is a shared understanding among all the stakeholders involved about the importance of the sector and the need to work together to build resilience. In Estonia, for instance, every Ministry and participating institution within the system designates an individual within their respective organization to act as a liaison in the event of an incident. Importantly, the Baltic states place great emphasis on institutional learning, which drives the constant evolution of their critical infrastructure protection system.

The implementation of the legislative framework for critical infrastructure protection in Kosovo must go hand in hand with **instilling a security culture within the institutional stakeholders** involved in the sector. As a starting point, a crucial component of this relates to **awareness raising** about the importance of securing critical infrastructures and the potential dangers associated with not doing so. One approach to achieving this is to have the MIA facilitate the participation of personnel from the Division for Critical Infrastructure in **international trainings, workshops, exercises,** and **conferences** delivered by experts in the field. In this way, they would gain valuable insights and knowledge about the latest trends, best practices, and emerging challenges in critical infrastructure protection. The Division can then leverage the expertise gained to deliver specialized training sessions for officials from the sectoral ministries involved in critical infrastructure protection. This allows for knowledge exchange between the various public stakeholders involved, which ultimately would contribute to fostering a security culture within these institutions.

Which institutional entity is assigned the **leading role in the field of critical infrastructure protection** is an important factor in ensuring an effective and coordinated protection of vital infrastructures. In the case of Latvia, the responsibility for national and EU-level critical infrastructure lies with the Cabinet of Ministers. Lithuania, on the other hand, has designated the Government as the leading entity in determining specific services and sectors as critical infrastructure. The lead agency for crisis management and continuity

of vital services in Estonia underwent a change from the Ministry of Interior to the Government Office in 2021.[29] The question of which institutional entity assumes a leading role in a sector is closely intertwined with the **strategic culture** prevailing in a country. In Kosovo, it is the Government Office who is the bearer of security-related national strategies. Subsequently, other institutional actors, such as ministries, often view Government office as a central coordinating body on security-related matters. However, in the case of Kosovo, the leading role in the critical infrastructure sector was assigned to the MIA. Considering that the critical infrastructure protection sector necessitates the active involvement of various sectoral ministries, it may be more productive for the Government Office to assume the leading role. This is because ministries are generally more receptive and open to receiving guidance from the Government Office rather than from another ministry, such as the MIA, in this context.

One challenge present in critical infrastructure systems in Latvia and Lithuania is the **complexity of the legal norms and organizational structure within the sector**. In Latvia, the critical infrastructure system is governed by multiple laws, overseen by several institutions, and operates within a broader framework of national security. In Lithuania, the two regulatory ecosystems for critical infrastructure protection mentioned above evolved separately from one another. This poses a significant challenge for subjects of critical infrastructure protection in these countries, as they may be required to adhere to instructions from multiple legal acts or supervisory institutions addressing essentially the same issue. Both Latvia and Lithuania are actively striving to **streamline their respective systems**, aiming to make them less entangled and more cohesive. A key takeaway point for Kosovo in this regard is to **establish a coherent and well-designed system from the ground up**, in order to avoid potential challenges and complications in the future. By setting up a clear system from scratch, Kosovo has the advantage of starting with a clean slate and proactively addressing emerging issues and vulnerabilities as they arise.

The number and type of vital services included in the legislation is an additional important aspect of critical infrastructure protection. This process should be driven by several factors, such as the geographic and demographic characteristics of a country, its economic and historical development, as well as internal and external threat perceptions. Importantly, there need to be systematically applied **criteria for the inclusion of certain objects or systems under the category of critical infrastructure**. While the process of identifying and designating critical infrastructure in the country is still pending, the legal framework in Kosovo has already established a comprehensive list of 11 critical infrastructure sectors, which include dangerous goods, energy, financial services, food and agriculture, government facilities and spaces, healthcare and public health, information and communication technology, national value, public services, transport, and water supply sewage. The inclusion of 'national value' as one of the critical infrastructure sectors can be a subject of debate and potential challenges, most notably in defining and prioritizing specific assets, objects, or systems within this sector. By expanding the scope of critical infrastructure to include objects related to national values, there is a risk of diluting the focus on core critical infrastructures that are essential for the functioning of society. Additionally, there is a risk that the concept itself may lose its significance and effectiveness.

Another aspect that Kosovo may need to reconsider in its current framework is placing more emphasis on the **protection of services rather than individual objects** that are of critical infrastructure. Estonia provides a good example in this respect, with its 'continuity of vital services' concept. This approach places a strong emphasis on ensuring the availability of essential services or their components as a key aspect of critical infrastructure protection. Additionally, it recognizes the interconnected nature of critical infrastructures and the need to safeguard their uninterrupted functioning.

Lastly, it is crucial for national authorities in Kosovo to allocate sufficient resources to **strengthen civil preparedness**. Two good examples in this respect are the 'Be Prepared!' application developed by the Women's Defense League in Estonia[30] and the 'Code of Conduct for Crisis Situations' published by Government Office in cooperation with Ministry of Interior and the Rescue Board.[31]

Both these resources contain valuable tips on how to respond to different emergency situations, such as during natural disasters, disruption of vital services and cyber security incidents. With minimal resources and a more proactive approach, Kosovo authorities too can develop similar tools and resources to strengthen civil preparedness in case of critical infrastructure disruptions.

Endnotes

1. European Council. "Impact of Russia's Invasion of Ukraine on the Markets: EU Response." Impact of Russia's invasion of Ukraine on the markets: EU response - Consilium (europa.eu).
2. Dolan, J. Chris. "Hybrid Warfare In The Western Balkans: How Structural Vulnerability Attracts Maligned Powers And Hostile Influence." SEEU Review 17, no. 1 (2022). seeur-2022-0018 (sciendo.com).
3. Kajosevic, Samir. "Western Balkans Urged to Prepare for Uptick in Cyber Attacks." Balkan Insight, September 12, 2022. Western Balkans Urged to Prepare for Uptick in Cyber-Attacks | Balkan Insight
4. "Albania quake toll hits 51 as search for survivors ends." DW.com, November 29, 2019. Albania quake toll rises to 51 – DW – 11/30/2019.
5. Zeqiri, Ardita. "Floods hit Kosovo, cutting drinking water supply to many towns." Prishtina Insight, January 19, 2023. Floods Hit Kosovo, Cutting Drinking Water Supply to Many Towns - Prishtina Insight.
6. "Safeguarding Critical Infrastructure in Kosovo." Kosovar Centre for Security Studies (2022). 1_Infrastruktura_Kritike_-_Eng.pdf (qkss.org)
7. Ibid.
8. Gadzo, Mersiha. "Fears simmer as an interethnic conflict brews in Kosovo." ALJAZEERA, June 8, 2023. Fears simmer as an interethnic conflict brews in Kosovo | Conflict News | Al Jazeera.
9. Council of the European Union. "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 (Text with EEA relevance)." Official Journal of the European Union, December 8, 2008. EUR-Lex - 32008L0114 - EN - EUR-Lex (europa.eu).
10. LAW NO. 06/L-014 ON CRITICAL INFRASTRUCTURE. ActDocumentDetail.aspx (rks-gov.net).
11. Ibid.
12. Andzans, Maris, et al. Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication (Riga: Latvian Institute of International Affairs, 2021). Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication (liia.lv).
13. "Data leak." DW, February 17, 2010. Data leak – DW – 02/17/2010.
14. Delfrate, Valentina. "2007 Cyber attacks in Estonia: a case study." (2021). (PDF) 2007 CYBER ATTACKS IN ESTONIA: A CASE STUDY (researchgate.net).
15. European Parliament. "European Critical Infrastructure – Revision of Directive 2008/114/EC." European critical infrastructure (europa.eu).
16. Sytas, Andrius. "Russian threat to Baltic security rising -Estonian intelligence report." Reuters, February 8, 2023. Russian threat to Baltic security rising -Estonian intelligence report | Reuters.
17. Andzans, Maris, et al. Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication (Riga: Latvian Institute of International Affairs, 2021). Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication (liia.lv).
18. National Defence Act – Riigi Teataja. National Defence Act–Riigi Teataja.
19. 19 Emergency Act – Riigi Teataja. Emergency Act–Riigi Teataja.
20. National Defence Act – Riigi Teataja. National Defence Act–Riigi Teataja.
21. Andzans, Maris, et al. Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication (Riga: Latvian Institute of International Affairs, 2021). Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication (liia.lv).

22. Republic of Lithuania Lw on the Protection of Objects of Importance to Ensuring National Security. IX-1132 Republic of Lithuania Law on the Protection of Objects of Importance to Ensuring National Security (lrs.lt)
23. REPUBLIC OF LITHUANIA SEIMAS RESOLUTION ON THE APPROVAL OF THE NATIONAL SECURITY STRATEGY. NATIONAL SECURITY STRATEGY (lrs.lt)
24. Law on the Protection of Objects of Importance to Ensuring National Security. Lithuania - Law on the Protection of Objects of Importance to Ensuring National Security | Investment Laws Navigator | UNCTAD Investment Policy Hub
25. "Cyber Security Council of Lithuania convened for the first time". L24.lt, July 25, 2015. Cyber Security Council of Lithuania convened for the first time (l24.lt)
26. Andzans, Maris, et al. Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication (Riga: Latvian Institute of International Affairs, 2021). Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication (liia.lv).
27. REPUBLIC OF LITHUANIA LAW ON THE BASICS OF NATIONAL SECURITY. VIII-49 Law on the Basics of National Security (lrs.lt).
28. Andzans, Maris, et al. Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication (Riga: Latvian Institute of International Affairs, 2021). Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication (liia.lv).
29. Ibid.
30. "Be prepared!" Naiskodukaitse. Be prepared! (naiskodukaitse.ee).
31. "Code of Conduct for Crisis Situations." The Ministry of the Interior and the

Katalogimi në botim – **(CIP)**

Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

005.7(496.51)(047

Elshani, Donika

What can Kosovo learn from the baltic states' approach to critical infrastructure protection? / Donika Elshani. – Prishtinë : QKSS, 2023. – 20 f. : ilustr. ; 28 cm.

ISBN 978-9951-842-11-2

About KCSS

Established in April 2008, the Kosovar Center for Security Studies (KCSS) is a specialized, independent, and non-governmental organization. The primary goal of KCSS is to promote the democratization of the security sector in Kosovo and to improve research and advocacy work related to security, the rule of law, and regional and international cooperation in the field of security.

KCSS aims to enhance the effectiveness of the Security Sector Reform (SSR) by supporting SSR programs through its research, events, training, advocacy, and direct policy advice.

Advancing new ideas and social science methods are also core values of the centre. Every year, KCSS publishes numerous reports, policy analysis and policy briefs on security-related issues. It also runs more than 200 public events including conferences, roundtables, and debates, lectures – in Kosovo, also in collaboration with regional and international partners.

A wide-range of activities includes research, capacity-building, awareness raising and advocacy. KCSS's work covers a wide range of topics, including but not limited to security sector reform and development, identifying and analyzing security risks related to extremism, radicalism, and organized crime, foreign policy and regional cooperation, and evaluating the rule of law in Kosovo.

This year, KCSS celebrated its 15th Anniversary. For more details about KCSS, you can check on the following official platforms:

qkss.org
securitybarometer.qkss.org

@KCSSQKSS
#KCSSQKSS

ISBN 978-9951-842-11-2