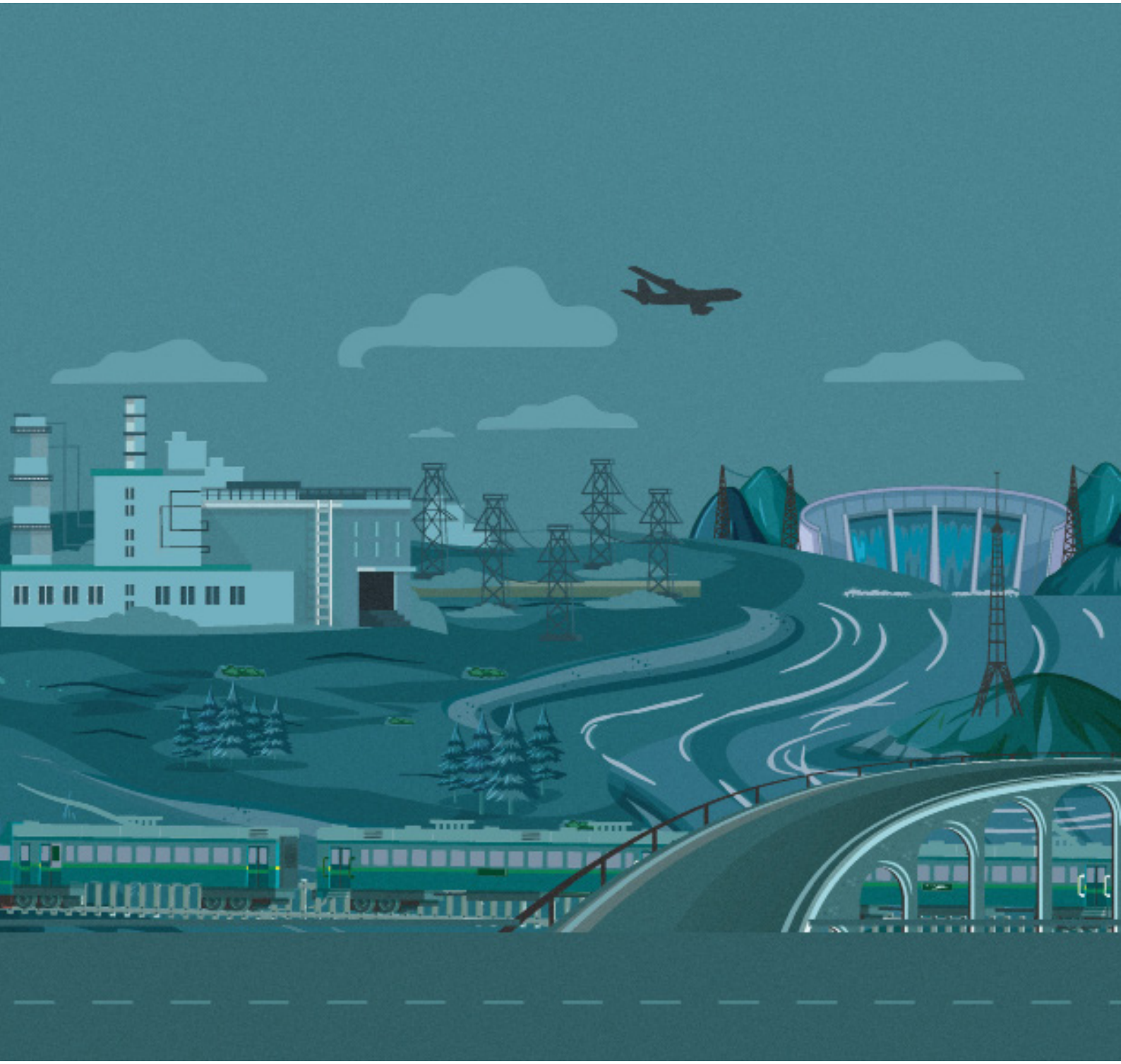
KCSS
Kosovar Centre for Security Studies

HOW CAN WE LEVERAGE FROM EUROPEAN PRACTICES TO ENHANCE CRITICAL INFRASTRUCTURE IDENTIFICATION IN KOSOVO?



Author: Jon Limaj

October: 2023

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

Author: Jon Limaj

Editors: Mentor Vrajolli
Ramadan Ilazi
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, critical infrastructure protection, hybrid threats and disinformation in Kosovo.

For more information, contact us

EmergingThreats@qkss.org

This policy brief is published in the framework of the SMART Balkans project, implemented jointly the 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

HOW CAN WE LEVERAGE FROM EUROPEAN PRACTICES TO ENHANCE CRITICAL INFRASTRUCTURE IDENTIFICATION IN KOSOVO?

October 2023

Table of contents

Executive Summary

In an era of rapid technological advancement, safeguarding critical infrastructure (CI) has become a matter of utmost concern for nations across the globe. The European Union (EU) defines critical infrastructure as threats to citizens' security and well-being. Strategically located in the Balkan region, Kosovo faces the all-important task of identifying and securing its critical infrastructure assets. Drawing insights from diverse methodologies, legislative frameworks, and collaborative strategies adopted throughout Europe, Kosovo aims to secure its critical infrastructure protection (CIP).

While Kosovo has regulated some aspects of its CI through sector-specific laws, the dedicated Law on Critical Infrastructure (LCI) was enacted in March 2018. This law defines critical national infrastructure, establishes criteria for identifying European critical infrastructure (ECI), outlines risk assessment and management procedures, and assigns roles and responsibilities for security coordination in this sector. Despite its promising intent, the LCI has faced challenges in the implementation process due to political crises, the pandemic, and government negligence.

Efforts to implement the LCI have gained traction in recent years, with steps taken to establish a dedicated Division for Critical Infrastructure (DCI) under the Ministry of Internal Affairs (MoIA). Harmonizing with evolving European legislation, particularly the EU-NIS Directive 2, poses an additional challenge. It advocates for accelerating LCI implementation and draws from European best practices to guide the identification and protection of critical infrastructure in Kosovo. Given Kosovo's sensitivity to both natural and man-made hazards, including floods, earthquakes, and security risks, fortifying CI resilience is vital.

Key provisions of the LCI mandate the development of operator security plans and the appointment of security coordinators. The limited resources of the newly formed DCI raise concerns about its operational capacity. International financial assistance, especially from the EU, is crucial to ensure effective protection measures. The EU's emphasis on safeguarding CI aligns with Kosovo's aim, and support in implementing the LCI can foster regional and European security collaboration.

In comparison to international models, Kosovo's CI sector remains in its inception phase. The identification of key sectors, alignment with European directives, and the need for cross-border protection reflect shared challenges. Successful frameworks from countries like the UK, Sweden, and EU member states can inform Kosovo's strategy to enhance CIP. Strengthening CIP in Kosovo demands a proactive implementation of the LCI, informed by international best practices. This effort aligns with the EU's commitment to secure CI resilience and contribute to regional security. By prioritizing CIP, Kosovo can bolster its national security, public safety, and overall societal well-being.

Context Analysis

Critical infrastructure (CI) is an "asset or system which is essential for the maintenance of vital societal functions, the damage, destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour of which may have a significant negative impact on the security of the EU and the well-being of its citizens".[1]

In our rapidly evolving world, the safety of CI has become a pressing concern for countries worldwide. Kosovo finds itself at a crossroad and is seeking effective strategies to identify and protect its vital infrastructure assets. Through exploring different methodologies, legislative frameworks, and collaborative approaches implemented across Europe, Kosovo can benefit by strengthening its CIP.

The protection of CI assets in Kosovo is not a novel concept. Throughout the years, there have been many different sector laws that regulate important aspects of CI without necessariy referring to it as such. These include, for instance, the Law on Interception of Electronic Communications, the Law on Electricity, the Law on Mines and Minerals, the Law on Waters of Kosovo, and the Law on Waste. While these sector-specific laws do regulate CI directly, many of them include provisions for the protection of CI assets within each respective sector. Nevertheless, the formal recognition of CI as a distinct sector with legal requirements for the government to establish centralized mechanisms and compile lists of both public and private critical assets is a relatively recent development.

Kosovo adopted the Law on Critical Infrastructure (LCI) in March 2018. [3] This law regulates the critical national infrastructure of the Republic of Kosovo and offers guidance for identifying infrastructures that qualify as European critical infrastructure (ECI). The law also identifies the sectors and criteria for identifying national and European CI and provides guidance for their management, including risk analysis, characteristics of safety plans for owners/operators, the roles and responsibilities of CI security coordinators, as well as fines for non-compliance.[3] LCI also provides a clear definition of CI as "an asset, system or part thereof necessary for the maintenance of vital and social functions, health, safety, economic or social welfare of the people, the disorder or destruction of which will have a significant impact on the Republic of Kosovo".[3] It is worth noting that this law aligns satisfactorily with the primary criteria established by European legislation, specifically the EU-NIS Directive 1. For a more comprehensive examination of the legal framework regulating CI in Kosovo and the implementation setbacks, please refer to the 2022 report by KCSS titled "Safeguarding Critical Infrastructure in Kosovo".

While it showed promise at the outset, the implementation of LCI has proven to be largely unfeasible. More specifically, the LCI mandated that within the initial 12 months, the Kosovo Government must establish a mechanism within the Ministry of Internal Affairs (MoIA), enact secondary legislation, and initiate the process of creating the list of CI. Despite some limited efforts, almost 5 years have elapsed since the adoption of the LCI and none of the afore-mentioned objectives have been accomplished. Several challenges have impeded the execution of the aforementioned actions, including the political and governmental crisis that spanned most of 2019-2021, the COVID-19 pandemic crisis (2020-2022), and the sustained governmental neglect since the law's adoption.

Indeed, since 2021 efforts towards the implementation of this law intensified to some extent. In late 2021, the MoIA temporarily appointed the head of the Division for Civil Aviation to initiate the establishment of a dedicated Division for Critical Infrastructure (DCI) under the Department

for Public Safety. In 2022, the MoIA published a new Organogram that outlined the structure of the DCI, which is expected to consist of six staff members, including the director of the DCI. Furthermore, in the last two years, there has been at least one documented effort by the Ministry to hire the head of the DCI and its supporting staff. It appears that due to the lack of professional qualities of candidates, this recruitment attempt has failed.

Aside from delays in its implementation, a consistent challenge is the alignment of the LCI with European legislation, which is a contractual obligation for Kosovo as stipulated by the Stabilization and Association Agreement (SAA). The EU has introduced the EU-NIS Directive 2, which differs significantly from the previous EU-NIS Directive 1. Kosovo's LCI was initially built upon the framework of the EU-NIS Directive 1. Notably, the EU-NIS Directive 2 not only refines the definition of CI but also includes provisions for essential infrastructure, which is not currently addressed in the existing law. Consequently, the implementation of the LCI may necessitate a comprehensive amendment process to align with the updated EU directive.

Taking into consideration this context, the purpose of this report is to advocate for increasing the dynamics of the implementation of the LCI, while also aiming to help the respective institutions learn from the European and regional best practices on what CI in the respective contexts means and how the process of CI identification should take place.

Understanding the Scale of Risks and the Importance of Enhancing CIP in Kosovo

Kosovo's CI faces various vulnerabilities, including natural and man-made threats. Geographically, the region is prone to hydro-meteorological challenges like floods, droughts, wildfires, and avalanches, as well as geophysical risks such as earthquakes and landslides. [4] Additionally, human negligence and deliberate actions, termed as security risks in this context, pose significant dangers. These risks encompass scenarios like dam failures, environmental pollution, water scarcity and industrial accidents, to name but a few. On the other hand, deliberate acts are another vulnerability for Kosovo, particularly in relation to risks of civil wars and cyber-crime. As elaborated in Table 1 below, a similar categorization of CI risks is provided by the LCI in Kosovo.

TABLE 1 ***Identified risks of the Critical Infrastructure in Kosovo:***

Natural risks

Hydro meteorological risks:

Climate-related hazards such as heatwaves and cold waves

Various types of floods such as flash floods, pluvial and fluvial floods

Droughts and wildfires

Avalanches, etc.

Geophysical risks:

Landslides and erosion

Earthquakes

Mass movement, etc.

Biological risks:

Epidemics, etc.

Man –Made risks and Technological risks

Water pollution and water scarcity

Dam security threats leading to dam failures

Air degradation and air pollution

Mining environmental degradation

Waste disposal leachate

Industrial leakages due to accidents

Security risks

Population density within Kosovo

Population migration

Political instability

Cyber-crime

Unscreened investments and corrosive capital

Supply chain threats

Emphasizing the need to identify CI as one of the initial necessary steps in the process of implementing the LCI, the report underscores that in Kosovo, this infrastructure extends beyond public ownership to encompass private ownership as well.[2] While there are laws protecting publicly owned infrastructure, their effectiveness is uncertain due to a lack of alignment with LCI, posing potential risks. The law defines a total of 11 CI sectors:[3]

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)

Water and wastewater (supply, reservoirs, and dams)

Implementing LCI requirements is a complex task. They require a lot of effort and commitment from institutions, especially when it comes to compiling the list of CI assets and developing the protection protocols or standard operation procedures for each respective CI sector. This has also been noted under Article 9 of the LCI, which states that an Operator Security plan must be developed, and should contain the identification and selection of all the needed measures to reduce the vulnerabilities and ensure the operation of all identified critical areas, facilities or network systems.

Additionally, as per Article 10 of the law, each sector designated as CI is mandated to appoint a Security Coordinator, with a representative from the Ministry of Interior serving as a Deputy Security Coordinator. In addition, operators of CI should appoint a Liaison Security Officer to act as a contact point for security issues as well as a connection between the operators/owners of national CI and ECIs. The MoIA has been designated as the contact point for the protection of ECIs as part of its supervisory role in implementing the LCI. It remains to be seen how this will play out once the law is implemented, given as the DCI is intended to be a relatively small unit, initially staffed only 6 members. It is worth noting that the scope of their responsibilities may be disproportionately extensive compared to the human resources available.

Kosovo remains in the early stages of developing its CI sector. A notable challenge lies in the limited available resources, as securing CI can entail substantial costs. Therefore, international financial assistance is crucial for effective CIP. This support can be extended within the framework of regional collaboration, with projects addressing the needs of the entire Western Balkans region. It's important to note that the EU places significant emphasis on safeguarding ECI, making regional efforts even more relevant and impactful. In this context, the LCI is harmonized with EU-NIS Directive 1 by incorporating the ECI within its framework and giving it significant importance. Just as the LCI defines it, the protection of the ECI is important because it includes the part of CI whose disruption or destruction would have a significant impact on at least two European countries. Hence, in principle, the protection of the CI is not only a domestic matter but also a regional and European one.

Why Does the EU Prioritize CIP and How Does It Identify CI?

The EU places significant emphasis on safeguarding CI due to its crucial role for national security, public safety, and economic stability. To prioritize the protection of CI and to ensure resilience, preparedness, and public confidence, the key CI sectors need to be identified.

Countries have different sectors whose assets, systems, networks, whether physical or virtual, are considered vital. In this regard, the US, for example, has identified 16 CI sectors, which include the chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defence industrial base sector, emergency services sector, energy sector, financial services sector, food, and agriculture sector, government facilities sector, healthcare, and public health sector, the information technology sector, nuclear reactors, materials and waste sector, transportation systems sector and water and wastewater sector. According to US legislation, "the destruction of any of these sectors would have a weakening effect on security, national economic security, national public health or safety".[5]

The Council Directive EC 2008/114 of the European Council defines ECI as any object, system or asset "the disruption or destruction of which would have a significant impact on at least two Member States." According to the same source, "damage and destruction of critical infrastructures by natural disasters, terrorism, and criminal activity may have a negative consequence for the security of the EU and the well-being of its citizens". [6]

EU member states have identified 10 indicative CI sectors such as energy, ICT, water, food, health, financial, public and legal order and safety, transport, chemical and nuclear industry, space, and research. The indicative list of the ECI sectors and their corresponding product or service is provided in the following table, [7].

TABLE 2 ***Indicative list of ECI sectors and corresponding product or service*** [7]

Sector	Product or service		
I. Energy	 *Oil and gas production, refining, treatment and storage, including pipelines*	 *Electricity generation*	 *Transmission of electricity, gas and oil*

II. Information, Communication Technologies, ICT	 *Information system and network protection*	 *Instrumentation automation and control systems (SCADA etc.)*	 *Internet*	 *Provision of fixed telecommunications*
	 *Provision of mobile telecommunications*	 *Radio communication and navigation*	 *Satellite communication*	 *Broadcasting*
III. Water	 *Provision of drinking water*	 *Control of water quality*	 *Stemming and control of water quantity*	
IV. Food	 *Provision of food and safeguarding food safety and security*			
V. Health	 *Medical and hospital care*	 *Medicines, serums, vaccines and pharmaceuticals*	 *Biolaboratories and bioagents*	

VI. Financial

Payment services/ payment structures (private)

Government financial assignment

VII. Public & Legal Order and Safety

Maintaining public & legal order, safety and security

Administration of justice and detention Civil administration

Government functions

Armed forces

Civil administration services

Emergency services

Postal and courier services

VIII. Transport

Road transport

Rail transport

Air traffic

Inland waterways transport

Ocean and short-sea shipping

IX. Space and Research

Space

Research

The prominence of these CI sectors in Europe stems from the fact that they have increasingly become targets of attacks in recent years. These increased attacks are mainly a result of outdated security protocols and weak security mechanisms.[8] The timeframe calculated from the system being breached by a malicious outsider until the breach is discovered and vulnerabilities are identified and patched is an average of 200 days.[9] The major CI systems in Europe that need to be protected are industrial, healthcare, and telecommunication systems.[10] The EU has a major objective of reducing the vulnerabilities of CI and increasing their resilience. At the EU level, 93 ECIs are identified, 88 of which are in the energy sector and 5 in the transport sector. Thus, the framework for all the activities that intend to improve CIP is given by the European Programme for Critical Infrastructure Protection (EPCIP).[11] This includes all relevant sectors of economic activity across all EU Member States.

In order to make ECI more secure, the European Commission has put forth a new approach to the EPCIP[12]. This enables new and more practical activities to be implemented for the prevention, preparedness, and response towards CIP and CI resilience. The EU directives do not impose specific mandatory methods or processes; instead, they establish the desired outcomes or results that must be achieved. For instance, even though the UK and Sweden do not have dedicated national legislation explicitly governing these aspects, they have established frameworks for the protection of CI. In contrast, countries such as Croatia, Greece, Hungary, Romania, and Bulgaria have enacted specific national laws designed to regulate and oversee CIP.

Recommendations for Enhancing the Resilience of Critical Infrastructure in Kosovo

Keeping in mind that each country's situation is unique, the recommendations should be tailored to the specific context and needs of each country. A holistic approach that combines technological solutions, policy development, and community engagement will be key to enhancing the resilience of CI in Kosovo.

Based on the above-mentioned challenges, the following recommendations should be considered:

- *Kosovo needs to urgently launch the process of drafting the essential policies and strategies for CI. However, for this to happen, the MoIA and the Government should consolidate the DCI immediately and adopt the respective secondary legislation and other policy documents that enable this process to kick off.*
- *Although there is a solid base in the LCI, it needs to be updated and harmonized with the newly adopted EU NIS Directive 2.*
- *Kosovo still needs support from the EU and international partners in effectively implementing the LCI. Additionally, it is advised that Kosovo advocates for and participates in regional projects led by the EU in protecting the ECI and CI, aimed at assisting Western Balkan countries in the formulation of legal frameworks and cooperative strategies.*
- *It is strongly recommended that Kosovo focuses on a pressing need to raise awareness among stakeholders about the importance of CI and the necessity of protecting it. This can be achieved through targeted awareness-raising campaigns and educational initiatives that inform various sectors and the public about the significance of CI.*
- *One of the main potential donors in this regard may be the EU. The EU needs to provide support to neighbouring and EU enlargement countries such as Kosovo in implementing the LCI.*
- *Kosovo should prioritize cross-sectoral cooperation and coordination among all stakeholders involved in CI management. This involves fostering collaboration between government agencies, private sector entities, local communities, and international partners.*
- *Kosovo needs to actively engage and integrate the private sector as a pivotal partner in advancing the resilience of CIs. The private sector is a catalyst for transformational changes in the CI sector. Private sector investments in CI resilience projects can be encouraged through incentives such as tax breaks, grants, partnerships, etc.*

- *Dynamic efforts in strengthening institutional capacity and training responsible officials through exercises, risk modelling, and scenario planning are highly needed. For this, it is vital for Kosovo to consider the insights and needs of local experts and communities. Incorporating local expertise ensures that initiatives and training are tailored to the unique challenges and opportunities in Kosovo.*

- *Taking into consideration the high vulnerability of the ECI and CIs to cyberattacks, sound ICT policies and actions need to be implemented and updated. This can be achieved by designing and applying ICT innovative solutions such as AI.*

Endnotes

1. Migration and home affairs, EU. https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en
2. Safeguarding critical Infrastructure in Kosovo. 2022. KCSS. https://qkss.org/images/uploads/files/1_Infrastruktura_Kritike_-_Eng.pdf
3. Law on Critical Infrastructure. 2018. https://www.kuvendikosoves.org/Uploads/Data/Documents/LigjinrO6L-014_RXXpkgUapT.pdf)
4. Kosovo security strategy (2022-2027). 2022. https://kryeministri.rks-gov.net/wp-content/uploads/2022/10/2-Strategjia-e-Sigurise-e-Kosoves-ENG.pdf https://www.kuvendikosoves.org/Uploads/Data/Documents/LigjinrO6L-014_RXXpkgUapT.pdf
5. Homeland security presidential directive 7. 2003. https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7
6. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of the European Critical Infrastructure and the assessment of the need to improve their protection. 2008. http://kemea.gr/images/documents/EC1142008CIP.pdf
7. Green paper on a European program for Critical Infrastructure protection. 2005. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.
8. Trend Micro, A Security Evaluation of AIS. 2015. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf
9. Info security, Hackers Spend 200+ Days Inside Systems Before Discovery. 2015. http://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/
10. A review of Critical infrastructure domains in Europe. 2021. https://www.spear2020.eu/News/Details?id=120
11. Commission staff working document, on a new approach to the EPCIP, making European critical infrastructure more secure. 2013. https://home-affairs.ec.europa.eu/system/files/2020-09/swd_2013_318_on_epcip_en.pdf
12. European Programme for Critical Infrastructure Protection (EPCIP). 2006. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

Katalogimi në botim – **(CIP)**
Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

005.7(496.51)(047)

Limaj, Jon
How Can We Learn from European and Regional Practices to Unlock the Process of Identifying Critical Infrastructure in Kosovo? / Jon Limaj. - Prishtinë : QKSS, 2023. - 11 f. : ilustr. 28 cm.

ISBN 978-9951-842-05-1

About KCSS

Established in April 2008, the Kosovar Center for Security Studies (KCSS) is a specialized, independent, and non-governmental organizate. 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 978-9951-842-05-1