



SAFEGUARDING CRITICAL INFRASTRUCTURE IN KOSOVO



**DECONSTRUCTING EXISTING
POLICIES AND PRACTICE**

© All rights reserved to Kosovar Center for Security Studies. Law on Copyright and Related Rights protects rights and intellectual property. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any forms or by any means, electronic, mechanical or other, without the permission in writing from the publisher. Commercial use of all media published by the Kosovar Center for Security Studies (KCSS) is not permitted without the written consent of the KCSS. Please contact: info@qkss.org or +383 38 221 420.



KCSS
Kosovar Centre for Security Studies

SAFEGUARDING CRITICAL INFRASTRUCTURE IN KOSOVO

DECONSTRUCTING EXISTING POLICIES AND PRACTICE

January 2022

TABLE OF CONTENTS

- EXECUTIVE SUMMARY 1

- INTRODUCTION 3

- I. EU POLICIES FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE..... 6

- II. LINKING THE CRITICAL INFRASTRUCTURE WITH OTHER SECURITY SECTORS.....9
 - 2.1. Civil emergencies 9

 - 2.2. Terrorism.....10

 - 2.3. Cyber Security11

 - 2.4. Private security services 13

- III. LEGAL REGULATION OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF KOSOVO...15
 - 3.1. The process of drafting the law on critical infrastructure 15

 - 3.2. Law implementation into practice 16

- IV. OPERATOR SECURITY PLAN AND SECURITY COORDINATORS 20

- CONCLUSION 22

EXECUTIVE SUMMARY

In 2018 the Republic of Kosovo adopted the Law on Critical Infrastructure, but which entered into force in April 2019, fully transposing the relevant legislation of the European Union. The law implements a comprehensive approach to risks, including risks and threats coming from terrorism, natural and other disasters. Critical infrastructure is any infrastructure that is vital to the functioning of a state. The drafting of the law is mainly based on EU legislation and best international practices.

Although the adoption of this law has put Kosovo one step ahead of other Western Balkan countries which have not yet adopted a similar law, its implementation into practice remains a challenge. The law has set deadlines for the implementation of the relevant provisions but they have not yet been implemented. The creation of the institutional framework is the main aspect for the implementation of the law, therefore the lack of its functionalization within the MIA has made the law on critical infrastructure not implementable and left the legal framework incomplete as the relevant bylaws, policies and standard operating procedures are missing. While there has been a greater institutional commitment to drafting the law, major delays in establishing the institutional mechanism and enforcing the provisions of the law reflect the lack of government institutions' will and commitment to implement it. The Government Program of Kurti II has planned identification and categorization of national critical infrastructure but has not envisaged any specific activity and indicators. It is important that MIA plans within its annual plan specific activities for implementation of the law.

Critical infrastructure protection is linked to several security policies such as: national security, defense strategy, civil emergencies, terrorism, cyber security and private security services. It is therefore necessary to update and finalize the legal and strategic framework by avoiding eventual overlaps between them.

KEY FINDINGS

▶ MIA has not yet established or functionalized the institutional mechanism within its structure, which is the first and main step in starting to implement the law, while no sub-legal act has been issued yet. On the other hand, the Government has not yet taken any actions in fulfilling its obligations deriving from the law.

▶ The new National Security Strategy, as the basic policy for security priorities, should treat the protection of critical infrastructure as one of its priorities and make a clear division of institutions' responsibilities and tasks as well as coordinate legal and strategic initiatives to ensure synergies between them.

- ▶ The Draft Defense Strategy should be reviewed in line with the new mandate of the KSF in order to protect the integrity and sovereignty, including the protection of critical infrastructure through concrete actions.
- ▶ In the field of civil emergencies, the National Response Plan and the Integrated Emergency Management System should be reviewed as soon as possible given that the deadline for their review has passed.
- ▶ In the field of terrorism, the new Counter-Terrorism Strategy must be reviewed to plan activities for the protection of critical infrastructure from terrorist attacks, including obligations under the Joint Action Plan on Counter-Terrorism signed with the EU.
- ▶ In the field of cyber-security, the draft law on cybersecurity and the new Strategy on cybersecurity should be finalized, paying special attention to avoid duplication of mechanisms and conflict of legal provisions with the law on critical infrastructure. The initiative for drafting the law on Security Measures for Networks and Information Systems shall be reviewed, which creates overlap with the Law on National Critical Infrastructure and draft law on Cyber Security.
- ▶ In the field of private security services, the finalization and adoption of the new law on private security services should proceed as soon as possible.

INTRODUCTION

Following the terrorist attacks in the US in 2001 and the increase in threats and dangers from terrorism, countries have started to design or advance the legal, institutional, and technical framework to protect the critical infrastructure from terrorist attacks. On the other hand, there are also threats and risks from natural and other disasters, therefore the protection of critical infrastructure requires a comprehensive approach to responding to threats and risks.

Critical infrastructure is any infrastructure, physical or virtual, which is essential for the performance of key functions in a country, such as health, safety, economy, social welfare, etc. The Republic of Kosovo has adopted the Law on Critical Infrastructure which entered into force in April 2019,¹ becoming the first country in the Western Balkans to adopt such a law and transpose the relevant EU legislation.

There is currently no globally approved definition but countries and international organizations define it quite similarly to each other. The Republic of Kosovo defines critical national infrastructure as “an asset, system or part thereof necessary for the maintenance of vital and social functions, health, safety, economic or social well-being of the people, the disruption or destruction of which would have a significant impact on the Republic of Kosovo.”² The law has defined a total of 11 critical infrastructure sectors, while the institution responsible for implementation and supervision is the Ministry of Internal Affairs. In general, most of the critical infrastructures are owned / operated by the private sector while a smaller part belongs to the public sector. Therefore, all infrastructures that meet the criteria to be defined as critical infrastructure, whether owned/operated by public or private sector, are mandatory for the implementation of this law.

The European Union, through its EU 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, a system or part of it located in the Member States which is essential for the maintenance of the vital social functions, health, safety, economic or social well-being of the people, the disruption or destruction of which would have a significant impact on a Member State as a result of failure to preserve those functions.”³ The European Critical Infrastructure (ECI) is defined as “critical infrastructure located in the Member States, the disruption or destruction of which would have a significant impact on at least two Member States.” The significance of the impact will be assessed in terms of cross-sectoral criteria. This includes the effects resulting from cross-sectoral dependencies on other types of infrastructure.”⁴

According to Directive 2008/114/EC, the process of identifying and defining ECIs will be

1 Law on Critical Infrastructure: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313>

2 Ibid

3 Directive 2008/114/EC <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>

4 Ibid

carried out through a “step-by-step” approach and as such it initially focuses on only two priority sectors: Energy and Transport together with their respective sub-sectors. Meanwhile, during the implementation evaluation process, the need for involvement of other sectors will be assessed.⁵




The United States defines critical infrastructure as “Systems and assets, whether physical or virtual, so vital to the United States that failure or destruction of those systems and assets would have a debilitating impact on security, national economic security, public health or safety or any combination of those issues.”⁶ Critical Infrastructure in the US consists of 16 sectors while the responsible institution is the Cyber Security and Infrastructure Security Agency.

The bellow table reflects the critical infrastructure sectors identified by the Republic of Kosovo, the EU and the US. (see next page)

⁵ Ibid.

⁶ American Patriot Act: <https://www.govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>

CRITICAL INFRASTRUCTURE SECTORS

 REPUBLIC OF KOSOVO		 EUROPEAN UNION		 USA	
1	Dangerous Goods	1	Energy	1	Chemical Sector
2	Energy	2	Electricity	2	Commercial Building Sector
3	Financial Services	3	Oil	3	Communication Sector
4	Food and Agriculture	4	Gas	4	Critical Manufacturing Sector
5	Government Facilities and Spaces	5	Transport	5	Dams Sector
6	Healthcare and Public Health	6	Road Transport	6	Defense Industrial Base Sector
7	Information and Communication Technology	7	Rail Transport	7	Emergency Services Sector
8	National Value	8	Air Transport	8	Energy Sector
9	Public Services	9	Inland Waterways Transport	9	Financial Services Sector
10	Transport	10	Ocean and Short-Sea Shipping and Ports	10	Food and Agriculture Sector
11	Water Supply and Sewage			11	Government Facilities Sector
				12	Healthcare and Public Health Sector
				13	Information Technology Sector
				14	Nuclear Reactors, Materials and Waste Sector
				15	Transportation Systems Sector
				16	Water and Wastewater System Sector

EU POLICIES FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE

Following the September 2001 terrorist attacks in the United States and the growing threat of terrorist attacks in Europe, in 2004 the European Commission issued a communication on the protection of critical infrastructure in the fight against terrorism.⁷ As a result, in 2006 the European Commission published the European Critical Infrastructure Protection Program,⁸ on the basis of which a legal framework would be created that would regulate the protection of European critical infrastructure through a Directive, the development of measures for the support of member states for critical national infrastructure, financial accompanying measures, etc.

In this regard, EU Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of critical European infrastructures and the assessment of the need to improve their protection was adopted.⁹ In 2019 the Evaluation of the Directive was published and a number of recommendations were given.¹⁰

According to the Evaluation Report of the Directive, as of August 2018 there are 93 ECIs identified.¹¹ Of the total number, 88 are in the energy sector while 5 in the transport sector. Most of the identified infrastructure is in the countries of Central and Eastern Europe, while about 60% of the total number is located in two member states.¹² Designated infrastructures and their location are classified information.

On December 5, 2018 at the EU-Western Balkans Ministerial for Justice and Home Affairs, representatives of the six Western Balkan countries and the European Commission signed a Joint Action Plan on Counter-Terrorism for the Western Balkans.¹³ The plan consists of five objectives which were planned to be implemented by December 2020.

While the first four objectives address the prevention and combating of terrorism and violent extremism, the fifth objective "Strengthening the protection of citizens and

7 EC Communication on the protection of critical infrastructure in the fight against terrorism:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=GA>

8 European Critical Infrastructure Protection Program: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN>

9 Directive 2008/114/EC: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>

10 EC assessment for Directive 2008/114/EC: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf

11 Ibid.

12 Ibid.

13 Joint Action Plan on Counter-Terrorism for the Western Balkans: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/docs/20181005_joint-action-plan-counter-terrorism-western-balkans.pdf

infrastructure”, has planned several joint measures and also obligations for each country and the EU as a whole.

This Plan creates some obligations for each country of the Western Balkans, while the following reflects only those related to critical infrastructure:

- Improving the protection of public spaces according to the European Action Plan to support the protection of public spaces and critical infrastructure;
- Improving the protection of cyberspace according to the EU Cyber Security Strategy and the NIS Directive.

On the other hand, the Plan requires the EU what within the external dimension of the European Program for the Protection of Critical Infrastructure, to continue inviting the countries of the Western Balkans to identify concrete projects and topics for cooperation, such as specialized training and to promote the exchange of good practices in workshops on protection of critical infrastructure.

Based on this Plan, the European Commission and each of the Western Balkan countries have signed the working agreement with the relevant obligations for the 2019–20 period, while the Republic of Kosovo signed the agreement in October 2019.¹⁴ According to the EU Office in Kosovo, based on this agreement, Kosovo should establish an institutional mechanism in the MIA, a mechanism for exchange of information between the public and private sector and the drafting of SOPs.¹⁵ As explained in more detail in Chapter III, these mechanisms have not yet been established or operationalized by the MIA.

Critical infrastructure protection is a relatively new area for the Republic of Kosovo and other Western Balkan countries, and they possess limited capacities to develop policies and implement them into practice. The case of Kosovo is a concrete example of how legislation was drafted with the support of development partners while implementation in practice faces many challenges due to lack of local capacity and lack of project to support implementation of the legislation.

Given that the protection of critical infrastructure has a transnational dimension and that other Western Balkan countries have not yet adopted an appropriate legal framework, it is necessary to involve the European Commission in providing assistance through both country-specific and regional projects to ensure a comprehensive approach of the Western Balkan countries to the protection of critical infrastructure. The involvement of the European Commission is necessary as we are dealing with the transposition of an EU directive that helps to harmonize national legislation with that of the EU, but the support of the European Commission is also a commitment stemming from the Joint Action Plan on Counter-Terrorism for the Western Balkans.

The protection of critical infrastructure is a segment which affects not only the maintenance of the vital functions of security, economy, health and welfare a country but also the regional and the European Union one. Taking into account the international interdependencies of infrastructures, the support of this field by the European Commission should be considered a priority regardless of the progress of the European integration process.

14 European Commission: https://ec.europa.eu/home-affairs/news/20191030_commission-authorities-kosovo-endorse-arrangement-counterterrorism_en

15 Interview with Visar Bivolaku, Policy Officer, EU Office in Kosovo, conducted via email on 18.01.2021

RECOMMENDATION 1

The European Commission to provide support to Kosovo in the implementation of the Law on Critical Infrastructure, but also regional projects focusing initially on supporting the Western Balkan countries in drafting the legal framework and creating modalities of cooperation. It is important that such projects take into account the primary role of institutions and local expertise and be in line with the local situation and needs.

II. LINKING THE CRITICAL INFRASTRUCTURE WITH OTHER SECURITY SECTORS

Government policies in the field of critical infrastructure protection stem mainly from the security sector, more precisely the Ministry of Internal Affairs as the bearer of this sector. The protection of critical infrastructure is one of the main areas of national security, and therefore the new National Security Strategy should include concrete sectoral and cross-sectoral actions in the field of legal, strategic, human and technological capacity. On the other side the draft Defense Strategy drafted by the Ministry of Defense does not include the protection of critical infrastructure although this should be the basis of any defense strategy. The Defense Strategy is one of the most important strategies at the country level after the National Security Strategy, so it is extremely important that this draft be improved and that this strategy also plans measures for its protection.

However, as these two key Strategies are still being drafted, the report will not focus on them. The focus of this report will remain on the existing strategic documents and policies which focus on the protection of critical infrastructure and which so far are concentrated on these 4 categories: civil emergencies, terrorism, cyber security and private security services.

RECOMMENDATION 2

The Draft Defense Strategy needs to be improved in accordance with the new KSF mandate in order to protect the integrity and sovereignty, including the protection of critical infrastructure through concrete actions.

2.1. CIVIL EMERGENCIES

The Emergency Management Agency is an executive agency within the MIA responsible for managing and protecting against natural and other disasters. The Government of the Republic of Kosovo in 2010 has adopted two policies which implement a comprehensive approach to responding to natural disasters and other incidents: National Response Plan¹⁶ and Integrated Emergency Management System.¹⁷ Both of these documents address the coordination of activities in the management of emergencies and incidents in general terms, including the critical infrastructure

¹⁶ National Response Plan: <https://ame.rks-gov.net/content/templates/ame/uploads/2020-10/Plani%20Reagimit%20Kombetar.pdf>

¹⁷ Integrated Emergency Management System: <https://ame.rks-gov.net/content/templates/ame/uploads/2020-10/SIME%20i%20Miratuar.pdf>

which is mentioned in many cases.

Based on the National Response Plan, MIA is responsible for reviewing and amending it every 4 years or more often as assessed by the Minister of the MIA. On the other hand, the Integrated Emergency Management System envisages its revision in the 2-year cycle. Only the documents approved in 2010 are published on the official website of the Office of the Prime Minister, MIA and EMA, which means that these two documents have not been reviewed. Therefore, taking into account the changes in the legal framework and policies, new threats and risks, there is a necessity to review both documents as soon as possible.

On the other hand, based on the Law on Protection from Natural and Other Disasters, in 2020 was approved the Government Regulation no.25/2020 on the methodology of drafting the risk assessment which has repealed the Government Regulation 28/2012 on the methodology of conducting the risk assessment.¹⁸ The new regulation obliges the drafting of the assessment by all legal entities that own or manage facilities or departments in which hazardous substances are present and legal entities whose activity is related to critical infrastructure facilities. Article 5 defines the integral parts of the assessment which are quite similar to Article 9 of the law on critical infrastructure. Furthermore, the regulation through Article 10 has regulated the assessment and consequences of critical infrastructure emphasizing that it should be based on the law on critical infrastructure.¹⁹ The implementer of this regulation should ensure that there is no overlap of this regulation with the law on critical infrastructure and in case it is encountered in practice then this regulation should be reviewed immediately. However, it would be preferable for this regulation not to address critical infrastructure at all, as this area is regulated by primary legislation. Furthermore, the issuance of this regulation has imposed additional obligations on its owners/operators and thus it creates duplications and causes confusion to the operators/owners.

RECOMMENDATION 3

To review the National Response Plan and the Integrated Emergency Management System as soon as possible, taking into account the current situation in the legal framework, policies, institutional framework as well as risks and threats. Also, urgently analyze the compliance of the Regulation on the methodology of developing risk assessment with the law on critical infrastructure as there are elements that can create overlap and cause confusion to operators/owners of critical infrastructure.

2.2. TERRORISM

The Government of the Republic of Kosovo has so far adopted three strategic documents with the aim of preventing and combating terrorism: the Strategy against Terrorism and the Action Plan 2009–2012, the Strategy against Terrorism and the Action Plan 2012–2017 and most recently the Strategy against Terrorism and Action

¹⁸ Government Regulation no.25/2020 on the methodology for drafting the risk assessment: <https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10293>

¹⁹ Ibid.

Plan 2018–2022. Protecting critical infrastructure from terrorist attacks is an integral part of the first two strategies but no concrete actions or measures planned are known as Action Plans are closed documents due to sensitivity.

In the first Strategy against terrorism 2009–2012,²⁰ the third pillar of the strategy, “Defense”, aimed, among other things, to reduce vulnerability and eliminate the possibility of terrorist attacks on critical infrastructure. This way, the specific objective set was: “Strengthening of the protection of critical infrastructure, facilities of special importance, places with high presence of people, institutions and authorities of local and international importance.”²¹

In the second Strategy which included the period 2012–2017,²² within the third pillar “Protection” was planned “protection of the citizens of the Republic of Kosovo, their property and protection of critical infrastructure from all terrorist acts.” Likewise, in pillar four “Preparation and Response” there is the activity of “Drafting defense plans and response scenarios for critical infrastructure and facilities of special importance.”²³

On the other side, Strategy Against Terrorism and Action Plan 2018–2023,²⁴ at least in the narrative part, contains no reference to the protection of critical infrastructure. However, this strategy is currently in the phase of merging with the strategy against violent extremism and so far the strategy has not yet been placed on the public consultation platform. However, the MIA, as the leader of this strategy, must plan actions to protect critical infrastructure from terrorist attacks, including the obligations arising from the Working Agreement for the implementation of the the Joint Action Plan on Counter-Terrorism for the Western Balkans, more precisely from the fifth objective.

In general, the concrete actions that are planned and implemented in the framework of counter-terrorism strategies in the field of critical protection are not known as the action plans are limited-access documents and not published. Kosovo Police has not responded to the questions regarding what actions have been taken by the Counter-Terrorism Directorate in protecting critical infrastructure from terrorist attacks.

RECOMMENDATION 4

The new strategy against violent extremism and terrorism should include concrete actions to protect critical infrastructure from terrorist attacks, including obligations under the Working Agreement on the implementation of the Joint Action Plan on Counter-Terrorism for the Western Balkans.

20 Strategy Against Terrorism 2008–2012: <http://www.kryeministri-ks.net/repository/docs/Strategjia>

21 Ibid.

22 Counter-Terrorism Strategy 2012–2017: http://www.kryeministri-ks.net/repository/docs/Strategjia_kunder_Terrorism_2012-2017.pdf

23 Ibid.

24 Strategy against terrorism 2018–2022: <https://mpb.rks-gov.net/Uploads/Documents/Pdf/AL/46/STRATEGJIA%20SHTET%C3%8BRORE%20KUND%C3%8BR%20TERRORIZMIT%20DHE%20PLANI%20I%20VEPRIMIT%202018%20%20E2%80%932023.pdf>

2.3. CYBER SECURITY

In January 2016 the Government of the Republic of Kosovo has approved the first Cyber Security Strategy and Action Plan 2016–2019²⁵ becoming at the time the second country in the Western Balkans after Montenegro to adopt such a strategy. This strategy has paid special attention to the protection of critical information infrastructure, setting it as the first strategic objective of the strategy. A specific objective within it is set for the “Identification of critical information infrastructure” while in the second strategic objective “Institutional development and capacity building” there is an objective to draft the Law on Critical Infrastructure.²⁶ In general, in this strategic document the term “critical infrastructure” is used extensively – 40 times. Currently, the MIA is drafting a new Strategy for Cyber Security which is not yet published on the public consultation platform. The new strategy should be drafted in line with the EU Cyber Security Strategy and continue to plan actions to protect critical infrastructure and critical information infrastructure.

On the other hand, in 2019 the Government approved the Concept Document on Security Measures for Networks and Information Systems which was drafted by the Ministry of Economic Development.²⁷ Based on the recommended option, it was planned to issue the Law on Security Measures for Networks and Information Systems and transpose Directive 2016/1148 regarding measures for a common high level of network and information systems security throughout the Union, otherwise known the NIS Directive. This concept document, among others, planned to give the Ministry of Economic Development the authority to monitor and coordinate activities in the network and information systems security measures used as critical infrastructure for the private and public sector. However, the content of this concept document, especially the proposal for drafting a separate law, created an overlap with the Law on Critical Infrastructure, where information and communication technology is one of the critical infrastructure sectors and as such covered by the applicable critical infrastructure law. Also this concept document created duplication and conflict between the competencies and authorizations of MIA and MED.

However, the draft law was not initiated by the MED and was not included in the Legislative Program of 2020²⁸ as in 2019 the MIA had started drafting the law on cyber security which also partially transposes the NIS Directive. Furthermore, Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222/JHA will be partially transposed²⁹ as well as the 2001 Council of Europe Budapest Convention on Cybercrime.³⁰ However, Government Kurti II in the Legislative Program

25 State Strategy for Cyber Security 2016–2019: https://www.kryeministri-ks.net/repository/docs/Strategjia_Shteterore_per_Sigurine_Kibernetike_dhe_Plani_i_Vepimit_2016-2019_per_publikim_1202.pdf

26 Ibid.

27 Concept Paper on Information Systems and Network Security Measures drafted by the Ministry of Economic Development: <https://kryeministri-ks.net/wp-content/uploads/2019/10/Koncept-Dokumenti-per-Masat-e-Sigurise-se-Rrjeteve-te-Sistemeve-te-Informahiya-shq.-1.pdf>

28 Legislative Program 2020: <https://kryeministri-ks.net/wp-content/uploads/2020/12/Programi-Legjislativ-p%C3%ABr-vitin-2020-i-p%C3%ABrdit%C3%ABsuar.pdf>

29 Directive 2013/40: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN>

30 Budapest Convention <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>

of 2021 has planned the drafting of the law on Security Measures for Networks and Information Systems, which creates overlap with the Law on Critical Infrastructure and draft Law on Cyber Security. The draft law on security has completed the public consultation process on August 11, 2020,³¹ while it has not proceeded for approval by the Government. Therefore, the MIA should finalize the draft law ensuring that there is no overlap between this draft law and the Law on Critical Infrastructure.

RECOMMENDATION 5

Adopt the cyber security law and the new cyber security strategy as soon as possible in line with the EU Cyber Security Strategy and relevant EU legislation, ensuring that there is no overlap of institutional oversight and conflict of legal provisions with the law on critical infrastructure. In addition, to review the initiative for drafting the law on Security Measures for Networks and Information Systems as it creates overlap with the Law on Critical Infrastructure and draft Law on Cyber Security.

2.4. PRIVATE SECURITY SERVICES

Private security companies offer their services based on Law no.04/L-004 on private security services³² which entered into force in 2011 and is the first law regulating this area. Pursuant to this law, the MIA licenses and authorizes companies to perform basic and specialized services. Currently, security services are provided in 5 areas: basic, close protection, cash transportation, electronic property surveillance, and securing public gatherings. As can be seen, the current legislation lacks the security service for critical infrastructure, but at the time of the adoption of the law on private security services, the legal basis for critical infrastructure was lacking. In practice, private security companies have been providing their services for infrastructure of various sectors such as energy, water supply, food, etc., which meet the criteria for being considered as critical infrastructure. This means that private security companies continue to provide security services for critical infrastructure, which have not yet been defined, and without completing any specialized training for the provision of these services thus endangering the assets and systems that provide vital services.

Therefore, in order to amend the above-mentioned law, in March 2016 the Government has approved the Concept Document for the regulation of private security services and since then the new law on private security services has not been adopted.³³ The draft law completed the public consultation on December 3, 2019³⁴ while it has

31 Draft law on cyber security: <https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=40905>

32 Law no.04/L-004 on private security services: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=2741>

33 Concept Document for the regulation of private security services: http://www.kryeministri-ks.net/repository/docs/Koncept-dokumenti_per_Rregimin_e_sherbjeve_private_te_sigurise_ne_Republiken_e_Kosoves_-_MPB.pdf

34 Draft Law on Private Security Services: <https://konsultimet.rks-gov.net/viewConsult>.

not yet been processed for approval by the Government. Based on the published draft, within the types of services, the security service for critical infrastructures has been increased by setting special conditions for companies that apply for licensed equipment for the provision of security services.³⁵ Establishing special conditions and criteria for licensing of private companies that provide security services for critical infrastructures is quite appropriate as it specializes the capacities of private companies in providing security services to critical infrastructures.

The adoption of this law is very important as private security companies provide security services to critical infrastructures, whether they are owned/operated by the public or private sector.

RECOMMENDATION 6

Finalize and proceed as soon as possible for approval of the new law on private security services, in order to specialize private security companies in providing security services to owners/operators of critical infrastructure.

php?ConsultationID=40820
35 Ibid.

LEGAL REGULATION OF CRITICAL INFRASTRUCTURE III. IN THE REPUBLIC OF KOSOVO

3.1. THE PROCESS OF DRAFTING THE LAW ON CRITICAL INFRASTRUCTURE

The process of legal regulation in the field of critical infrastructure protection was initiated by the MIA in 2014 through the drafting of the Concept Document for the Identification and Protection of Critical Infrastructure, which was approved by the Government of the Republic of Kosovo in 2015. This Concept Document has implemented a comprehensive approach to threats and risks, including those from terrorism, natural disasters and other incidents.

In analyzing this issue, the working group relied mainly on the European Critical Infrastructure Protection Program and Directive 2008/114/EC. In conclusion, as a recommended option, it is proposed to draft a special law on critical infrastructure, an option approved by the Government.

On the other hand, the drafting of the law on critical infrastructure had started in 2016 under the leadership of the MIA. The Working Group was composed of all central sector institutions which have responsibilities in the various critical infrastructure sectors as well as international development partners.

The Law on Critical Infrastructure was drafted by combining three approaches or concepts: 1) the EU concept mainly through Directive 2008/114/EC but also the relevant publications of the European Commission; 2) the Croatian concept through its Law on Critical Infrastructure³⁶ and 3) the USA concept through the American Patriot Act.³⁷ The Croatian concept has dominated the content of the law as it has regulated both its national critical infrastructure as well as European. Moreover, in many cases the laws in the Republic of Kosovo have been drafted based on the Croatian experience.

Directive 2008/114/EC which deals with ECI creates legal obligations only for EU member states. However, as some EU countries have not had a legal act on national critical infrastructure in force, during the transposition of this Directive both the critical national and European infrastructure has been regulated, as in the case of Croatia. Candidate and potential EU member states have no obligation to transpose the Directive. However, the Republic of Kosovo was the first to transpose this Directive through a special approach which will be explained below.

36 Croatian law on critical infrastructure: <https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama>

37 American Patriot Act: <https://www.govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>

Initially, based on the Croatian experience and Directive 2008/114/EC, the protection of critical national infrastructure was regulated through five articles of Chapter II. More specifically, it regulated what critical national infrastructure include, the sectors, the process of identifying and the listing the national critical infrastructure. Since most of the critical infrastructures are owned/operated by the private sector, a special article has been drafted on public-private cooperation through which the Government should provide various forms of support to the private sector, including financial incentives for owners/operators of infrastructure designated as critical infrastructure.

Chapter III sets out the content of the Operator Security Plan and the role of Security Coordinators and Liaison Officers, which is mainly based on Directive 2008/114/EC and the Croatian law.

Chapter IV regulates the European critical infrastructure where the lawmakers have shown a creative approach to be explained below. Whereas Directive 2008/114/EC defines the European critical infrastructure as "critical infrastructure located in "member states," the disruption or destruction of which would have a significant impact on at least "two member states," the law compiler replaces the words "member state" with "European country." Thus, the EU member states as well as the countries of the Western Balkans and other European countries are included.

Considering that the Republic of Kosovo is bordered by non-EU countries, there are critical infrastructures in the energy and transport sector which are located in the Republic of Kosovo, the disruption or destruction of which would have a significant impact on at least two other Western Balkans countries. Similarly, there are critical infrastructures found in other Western Balkan countries whose disruption or destruction would have a significant impact on at least two other states. However, in order to define European critical Infrastructure, the Western Balkan countries need to transpose Directive 2008/114/EC into their national legislation.

Chapter V regulates the process of monitoring and evaluating, supervision, handling sensitive information, and penalty measures. This chapter is based on Directive 2008/114/EC while the provisions on penalty measures are taken from the Croatian law.

3.2. LAW IMPLEMENTATION INTO PRACTICE

There is broad agreement that the Republic of Kosovo has a fairly advanced legal framework but its implementation in practice remains deficient or followed with challenges. The situation is similar with the Law on Critical Infrastructure which is so far unimplementable.

According to the response of the EU Office in Kosovo, from October 29 to November 1, 2019, the first mission of EU experts was realized who helped draft the National Plan for the Protection of Infrastructure in Kosovo. The second mission was scheduled for March 23-27, 2020 which due to the pandemic has been postponed indefinitely.

³⁸ It is important that this mission of experts is realized as soon as possible, even

³⁸ Interview with Visar Bivolaku, Policy Officer, EU Office in Kosovo, conducted via email on 18.01.2021

through electronic platforms, in order to start with the implementation of the above Plan drafted for the purpose of law enforcement.

The legal provisions which have a definite time limit and require special attention will be presented below:

National Critical Infrastructure

Pursuant to Article 4, the MIA is obliged to establish an institutional mechanism within its framework three (3) months after the entry into force of the law. This means that this mechanism should have been established in July 2019. On December 19, 2020, the Government approved the new regulation on Internal Organization and Systematization of Positions in the MIA,³⁹ where the Division for Critical Infrastructure will be created within the Department for Public Safety, in which a total of six (6) officials will work. It now remains for this mechanism to be completed with relevant and professional officials as well as to take measures for its full functionality including the necessary budget and working conditions.

According to paragraph 2 of this article, this mechanism will be responsible for drafting policies for the national critical infrastructure, providing guidance for the protection of critical infrastructure, exchanging information for the protection of critical infrastructure and leading projects for the protection of critical infrastructure.

The establishment and full functioning of the institutional mechanism is the main basis in terms of implementation of the law, as the entire law remains unimplementable until this mechanism is operationalized.

RECOMMENDATION 7

To urgently establish and functionalize the institutional mechanism within the MIA, allocating a necessary budget and engaging professional officials, and to start immediately with the training of officials and the drafting of bylaws and other relevant documents.

Critical infrastructure sectors

Article 5 lists 11 sectors that constitute the national critical infrastructure but other sectors can be added to this list through a Government Decision. Pursuant to this article, the Government must designate a sector coordinator in each relevant ministry or institution that has legal and institutional responsibilities over the sector.

The appointment of the relevant ministry or institution to exercise the role of coordinator is very important for the process of identifying critical infrastructure, defining cross-sectoral and sectoral criteria and coordinating activities for the protection of critical infrastructure within the relevant sectors.

³⁹ Regulation (OPM) - No. 01/2021 on Internal Organization and Systematization of Jobs in the MIA: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=36587>

RECOMMENDATION 8

The Government should issue as soon as possible a decision on the appointment of relevant ministries or institutions to exercise the role of the sector coordinator, while MIA in cooperation with the Coordinators should prepare the Work Plan and the Joint Plan for each Sector.

Identification of national critical infrastructure

Based on Article 6, the process of identifying critical infrastructure is led by the MIA in cooperation with other security institutions, governmental and non-governmental institutions, public and private owners and operators, as well as key international actors.

Further, it is noted that the identification process will be based on a comprehensive risk analysis, dependant on sectoral and cross-sectoral criteria, which must be finalized within six (6) months after the entry into force of this law. So, this document should have been finalized by October 2019.

It is assumed that the document with cross-sectoral and sectoral criteria has not yet been drafted as the relevant mechanisms have not been established. The drafting of this document and the whole identification process depends on when the institutional mechanism within the MIA will be functionalized, as it will be a unit responsible for leading this process.

The process of identifying critical infrastructure is one of the most important actions for implementation of the law and in planning measures for their protection by both security agencies and their owners/operators. Once the process of identifying critical infrastructures is complete, then the process of identifying them begins as stipulated in Article 7.

RECOMMENDATION 9

Start as soon as possible with the drafting of cross-sectoral and sectoral criteria in cooperation with relevant institutions and with the help of national and international experts, as well as address with priority the process of identifying infrastructures that meet cross-sectoral and sectoral criteria.

Designation of national critical infrastructure

Following the completion of the process of identifying and prioritizing the list of national critical infrastructure, according to Article 7 the Government, based on the proposals of the MIA, approves the list of national critical infrastructure, which is reviewed on annual basis and is a secret document. Within seven (7) days the MIA notifies the owners/operators of critical infrastructure, who should not disclose this notice to the public.

As noted above, critical infrastructure must first be identified and a list of proposals submitted for approval by the Government. The lack of approval of the critical

infrastructure list affects not only the security of a particular critical infrastructure but also the national security as a whole. The list of critical infrastructure would influence the security institutions to focus on their protection on the one hand, and the owners/operators of critical infrastructure on the development and implementation of security measures on the other.

RECOMMENDATION 10

Urgently prioritize, finalize and approve the list of critical infrastructure ensuring full implementation of the obligations of owners/operators for their maintenance.

Public-private cooperation

Most of the critical infrastructure is privately owned or operated. Therefore, public-private cooperation is one of the key ways of protecting critical infrastructure.

According to Article 8, the Government through the MIA has undertaken to provide various forms of cooperation and assistance to the private sector, which includes the exchange of information, the provision of training, etc.

Furthermore, the Government has foreseen financial incentives for owners/operators of infrastructure set as critical. This issue should be regulated through a sub-legal act which defines the form and criteria for providing financial incentives to owners/operators.

There is no information that work has been done on drafting any bylaw or other documents that lay the foundation and strengthen public-private cooperation in the field of critical infrastructure.⁴⁰

RECOMMENDATION 11

Immediately start with the drafting and approval of a sub-legal act by the Government to determine the conditions and criteria for providing financial support to owners/operators of critical infrastructure.

⁴⁰ KCSS has sent questions to the MIA regarding this issue but no response has been received.

OPERATOR SECURITY PLAN AND SECURITY IV. COORDINATORS

Operator Security Plan

Pursuant to Article 9, all owners/operators of designated critical infrastructure must develop an SOP or equivalent plan within nine (9) months of receiving the Government decision. This article sets out specific criteria for the content of the SOP in preventing and protecting critical infrastructure from accidents or incidents as well as in ensuring the continuity of work and the provision of services and goods. The content of the SOP is reviewed and approved by the MIA, EMA and the relevant ministry or institution for the relevant sector.

Where required, the MIA will provide support in drafting SOPs. However, the implementation of this article is followed with challenges as the authority to review and approve SOPs has not yet been established: the MIA has not functionalized the institutional mechanism while the Government has not yet designated relevant ministries or institutions as Sector Coordinators. On the other hand, no trainings have been held by the relevant authorities on drafting and reviewing SOPs. Therefore, public authorities will not be able to provide professional support to owners/operators in drafting SOPs.

RECOMMENDATION 12

Create and functionalize as soon as possible the authority to review and approve SOPs, including its training, and organize of trainings for owners/operators for the design and maintenance of SOPs.

Security coordinators and security liaison officers

According to Article 10, the relevant Ministry or institution appointed as the Sector Coordinator by the Government must appoint a representative to exercise the role of Security Coordinator while the MIA meets the role of Deputy Coordinator. The appointment of both positions should have been done within three (3) months after the entry into force of the law, which so far has not been accomplished. Critical infrastructure owners/operators, on the other hand, must appoint a security liaison officer.

Coordinators and Deputy Coordinators exercise an extremely important role as they are responsible for ongoing cooperation with security liaison officers and coordination of actions in the protection and security of critical infrastructure. The positions of Coordinators and Deputy Coordinators have not yet been filled by public institutions,

while security liaison officers have not been appointed as the Government has not yet issued a decision on the definition of critical infrastructure.

RECOMMENDATION 13

Relevant ministries or institutions and the MIA should appoint their representatives as soon as possible to exercise the function of Coordinators and Deputy Coordinators.

European Critical Infrastructure

As explained earlier, in order for an infrastructure to be considered as European critical Infrastructure, the basic criterion must be met for the impact from its destruction or disruption to affect at least two countries.

According to Article 11, the energy and transport sectors, including their respective sub-sectors, are designated as priorities but other sectors, depending on the situation and need, are not excluded. In the Western Balkans region there are critical infrastructures in the energy and transport sector whose disruption or destruction would affect at least two other countries. However, since the other countries of the Western Balkans have not transposed the Directive 2008/114/EC, the Republic of Kosovo cannot request the designation of any infrastructure located either in the Republic of Kosovo or any other country as a European critical infrastructure. However, the MIA should identify such infrastructures and ask the European Commission to engage more actively in this area by requesting the countries of the Western Balkans to adopt the legal framework.

RECOMMENDATION 14

MIA to engage in the identification of European Critical Infrastructure, either located in the territory of the Republic of Kosovo or in any of the Western Balkan countries and to seek support from the European Commission in defining those infrastructures as ECI after these countries adopt their own critical infrastructure law.

Bylaws

Pursuant to Article 22, the MIA must issue bylaws within six (6) months from the entry into force of this law. So far, the MIA and the Government have not drafted or finalized any bylaws. Bylaws are extremely important as they assist in the implementation of the law and their absence makes the legislation in the field of critical infrastructure be incomplete and unimplementable.

RECOMMENDATION 15

MIA urgently to start drafting relevant bylaws and approve them.

CONCLUSION

This analysis provided a detailed overview of the protection of critical infrastructure in the Republic of Kosovo, becoming the first document published in this field. While the MIAr has done a very good job in drafting the law on critical infrastructure, putting Kosovo one step ahead of other Western Balkan countries, the law remains unimplementable for almost 2 years following the date of its entry into force.

Critical infrastructure is a segment which is related to several other areas of security and defense, namely some strategic and legal documents which are in force as well as some new initiatives. Initially, strategic documents that are in the process of being drafted such as the draft National Security Strategy, the draft Defense Strategy, the draft Counter-Terrorism Strategy and the draft Cyber Security Strategy should include the protection of critical infrastructure by ensuring coordination of actions and by avoiding duplication or overlap of actions. The Strategic Planning Office within the Office of the Prime Minister should coordinate this process in cooperation with the relevant ministries. On the other hand, the draft law on cyber security should pay attention to the drafting of legal provisions which may cause overlap with the law on infrastructure, while the initiative for drafting the law on Security Measures for Networks and Information Systems needs to be reviewed. Moreover, the draft law on private security services should be finalized as soon as possible.

The analysis has shown that the Division for Critical Infrastructure in the MIA has not been established or functionalized yet, therefore this is the first step that should be done in order to implement the law. It is evident that public institutions have very limited capacities in the field of critical infrastructure, but they have had enough time so far to secure support from the European Union or other donors, but have failed to provide any projects. However, the support received from the TAIEX instrument should be used more until a more stable and long-term support is provided. Due to limited capacity and complexity of the field, external support should be ensured as soon as possible to provide training to relevant officials.

MIA, after functioning the mechanism within its structure, must urgently start cooperating with the Office of the Prime Minister, ministries and relevant institutions in preparing a detailed plan for implementing the law and the drafting of bylaws.

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

004:007
342.742
343

Politikat e qeverisë në mbrojtjen e infrastrukturës kritike. - Prishtinë : Qendra Kosovare për Studime të Sigurisë, 2021. - 23 f. ; 24 cm.

Mbrojtja civile
Krimet kompjuterike
Parandalimi

ISBN 978-9951-799-35-5

Aleph [000097651]



ISBN 978-9951-799-35-5



9 789951 799355