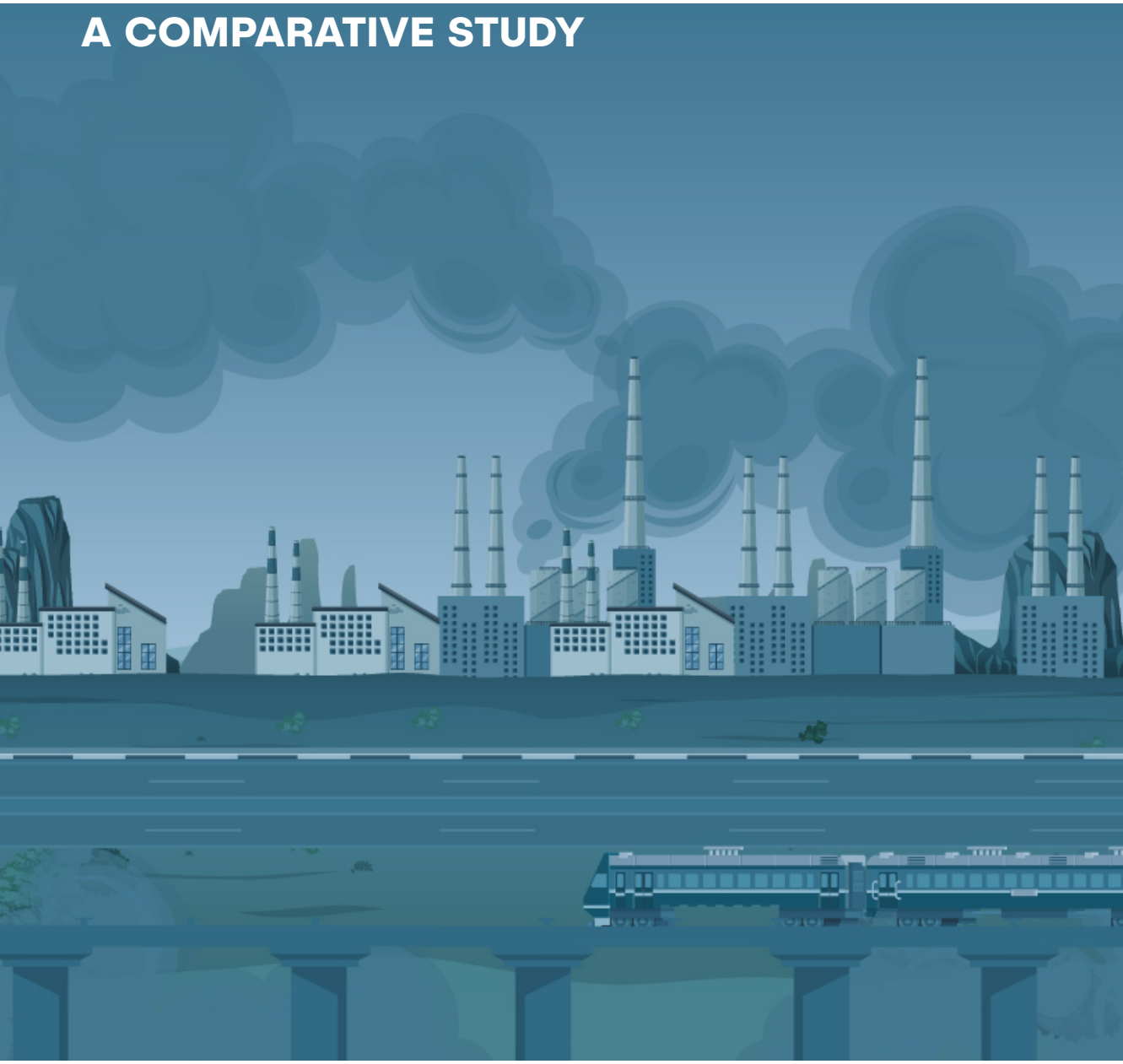
KCSS
Kosovar Centre for Security Studies

EMERGING THREATS PROGRAMME

ALIGNING KOSOVO'S CRITICAL INFRASTRUCTURE LAW WITH THE EU'S DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES AND EU'S NIS2 DIRECTIVE

A COMPARATIVE STUDY



January 2024

EMERGING THREATS PROGRAMME

Author: Besnik Limaj is a highly experienced **Team Leader** and **Cybersecurity Key Expert**, with a career spanning over 25 years in cybersecurity and software engineering.

He has held various **Team Leader roles in several EU** and other donor funded projects, including the multi-million Euro, three year **Cybersecurity East project for the six Eastern Partnership Countries (EaP)**. He also served as a Team Leader in the three year "**Enhancing Cyber Security - ENCYSEC**" transregional EU project for four countries in Europe and Asia. Additionally, he has also led an EU-funded project in Amman, Jordan, and served as a Key Expert for projects in Africa, Central, and South America.

Besnik's profound contributions include establishing over 15 CERT/CSIRTs **worldwide**, developing cybersecurity strategies, legislating cyber laws, and organizing comprehensive training and cyber exercises. Recognized for his active participation in Cyber Security Conferences, Besnik has in-depth knowledge of legal frameworks such as the EU NIS and CER Directive. Additionally, he is well-versed in key cybersecurity standards and guidelines, including the NIST Cybersecurity Framework and ISO 27001. His technical skills span Ethical Hacking, Metasploit, OSINT, Social Engineering, and Penetration Testing, combined with expertise in Python, SQL Servers, Oracle, and Data Science.

He has collaborated with international bodies such as ENISA, Council of Europe, and engaged with institutions including FIRST, Trusted Introducer, ITU, and TERENA/GÉANT. His work also extends to regional entities like AU, ECOWAS, EAC, COMESA, and SADC, collectively enhancing global cybersecurity practices.

Besnik has travelled the world and gained exposure to diverse people and cultures from Hong Kong to San Francisco.

He remains dedicated to advancing cybersecurity, continually seeking to enhance his knowledge and impact in the field.

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

ALIGNING KOSOVO'S CRITICAL INFRASTRUCTURE LAW WITH THE EU'S DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES AND EU'S NIS2 DIRECTIVE

A COMPARATIVE STUDY

January 2024

TABLE OF CONTENT

EXECUTIVE SUMMARY

This research document presents a thorough analysis and strategic recommendations for the revision of Kosovo's Law No. 06/L –014 on Critical Infrastructure. The objective is to align it with the latest European Union standards as defined in Directive (EU) 2022/2557 on the resilience of critical entities and the EU NIS 2 Directive 2022/2555, focusing on cybersecurity.

KEY OBSERVATIONS:

1. Legislative Context and Evolution:

- Kosovo's existing legislation, Law No. 06/L –014, initially aligned with the EU Directive 2008/114/EC, is now outdated due to the repeal of this directive and the advent of new EU standards.
- The new Directive (EU) 2022/2557 introduces a paradigm shift from a protection-centric to a resilience-centric approach, expanding the scope of critical infrastructure protection.
- The EU NIS 2 Directive 2022/2555 significantly broadens the cybersecurity framework, emphasizing the need for comprehensive risk management, enhanced incident reporting, and expanded sectoral coverage.

2. Comparative Legislative Analysis:

- The current Kosovo law focuses primarily on energy and transport sectors with defined roles for infrastructure protection, such as Security Coordinators and Security Liaison Officers.
- In contrast, the EU directives propose an integrative risk management approach, encompassing a wider array of sectors, including digital infrastructure, healthcare, and public administration, and stress the importance of EU-wide collaboration and information sharing.

3. Strategic Recommendations for Law No. 06/L –014:

- Revise the law to align with the resilience-oriented framework of Directive (EU) 2022/2557, emphasizing a comprehensive approach to risk assessment and management.
- Expand the sectoral scope to encompass critical sectors identified in the EU directives, ensuring comprehensive coverage of all vital infrastructure components.
- Enhance security and resilience planning, improve coordination mechanisms, and ensuring robust reporting and information exchange systems.

- Integrate cutting-edge cybersecurity technologies and practices, adhering to European cybersecurity standards and certification requirements.
- Foster robust international cooperation for knowledge sharing and collaborative efforts in infrastructure protection.
- Establish a mechanism for continuous review and dynamic adaptation of the law to respond effectively to evolving technological and threat landscapes.

Conclusion: The proposed alignment of Kosovo's critical infrastructure law with the EU's latest directives is imperative for Kosovo's continued infrastructural resilience and security. Implementing these strategic recommendations will ensure that Kosovo not only complies with EU standards but also enhances its capabilities to protect against modern threats. This progressive alignment will strengthen Kosovo's infrastructure resilience, thus securing the well-being and stability of its citizens in an increasingly interconnected and digitalized global environment.

OVERVIEW OF KOSOVO'S CRITICAL INFRASTRUCTURE LAW NO. 06/L -014

Law No. 06/L –014 on Critical Infrastructure in Kosovo, promulgated by Decree No.DL-016-2018, dated 20.04.2018, establishes a comprehensive legal framework for the protection and management of critical infrastructure in the Republic of Kosovo. Initially aligning with European Union standards, specifically the EU Directive 2008/114/EC of 8 December 2008, this law is instrumental in safeguarding national and European critical infrastructures, thereby ensuring the welfare and stability of Kosovo and its citizens.

However, it is important to note that the EU Directive 2008/114/EC, which formed the basis for this law, has been repealed and replaced by the new Directive (EU) 2022/2557 on the resilience of critical entities. This new EU Directive presents updated and more current standards and practices for the management and protection of critical infrastructures. Therefore, while Law No. 06/L –014 was comprehensive and aligned with EU standards at the time of its enactment, it is now recommended to urgently revise and update it to align with the new Directive (EU) 2022/2557, ensuring its relevance and effectiveness in the current context of critical infrastructure management.

The law is structured into five chapters and two annexes, each addressing different aspects of critical infrastructure management.

CHAPTER I

Chapter I of Law No. 06/L –014 on Critical Infrastructure sets the foundation for the protection and management of critical infrastructure within the Republic of Kosovo, aligning with European Union standards. It emphasizes the law's purpose to protect national and European critical infrastructure, safeguarding the welfare and stability of Kosovo and its citizens. The scope of the law is broad, covering the identification and management of national and European critical infrastructure, including the establishment of sectors, criteria for designation, and guidelines for their effective management. This includes the creation of safety plans, risk analysis, and the assignment of roles and responsibilities, such as Security Coordinators and Security Liaison Officers.

The chapter also provides detailed definitions of key terms and concepts, ensuring clarity and uniformity in understanding the law's provisions. These definitions range from the approach to hazards, roles of various coordinators and officers, to the categorization of infrastructures at both national and European levels. By establishing these parameters, the law seeks to protect critical infrastructures against a range of threats, ensuring their resilience and the continuous provision of essential services to the population.

CHAPTER II

Chapter II of Law No. 06/L –014 focuses on the regulation of National Critical Infrastructure in the Republic of Kosovo. It defines the critical infrastructure as vital systems and assets essential to the nation's security, economy, and public health. The Ministry of Internal Affairs (MIA) is tasked with establishing an institutional mechanism for implementing this law, serving as the main contact point for all critical infrastructure protection matters.

The chapter outlines the division of National Critical Infrastructure into various sectors, such as energy, healthcare, and transportation, to facilitate cooperation and management. It grants the Government, advised by MIA, the authority to designate additional sectors and appoint sector coordinators.

Identification of National Critical Infrastructure is a comprehensive process led by MIA, involving a risk analysis based on global threats and hazards. This process considers a range of criteria, including the impact of potential disruptions on various aspects like public health and the economy.

The Government, following MIA's proposals, designates National Critical Infrastructure. This designation is communicated confidentially to the relevant owners/operators, who bear direct responsibility for its protection and management. The list of designated infrastructures is kept classified and is reviewed annually.

The chapter also emphasizes the importance of public-private cooperation in ensuring the security and resilience of critical infrastructures. It mandates the Government, through MIA, to organize engagements and facilitate information sharing between public and private entities. Additionally, financial incentives are provided to owners/operators of designated critical infrastructure to strengthen their protective measures. This comprehensive approach underscores the law's commitment to securing Kosovo's vital systems and assets against a multitude of threats.

CHAPTER III

Chapter III of Law No. 06/L –014 addresses the Operator Security Plan (OSP) and the roles of Security Coordinators and Security Liaison Officers in the context of National and European Critical Infrastructure.

Owners and operators of designated critical infrastructure are mandated to develop and submit an OSP to the Ministry of Internal Affairs (MIA) within nine months of their designation. The OSP must encompass various security measures, including risk analysis and mitigation strategies. MIA provides technical assistance in developing these plans and reviews OSPs for compliance. In cases where OSPs are developed prior to formal designation, they are subject to review and potentially require revisions to meet the law's standards.

The chapter further outlines the establishment of Security Coordinators and Security Liaison Officers. Each critical infrastructure sector is required to appoint a Security Coordinator, assisted by a Deputy Coordinator from MIA, to coordinate protection activities within their respective sectors. These coordinators are responsible for collaborating with Security Liaison Officers, who are appointed by the owners/operators of the designated infrastructure. The Security Liaison Officer serves as the primary contact for security-related issues and facilitates communication between the infrastructure's management

and the security coordinators.

To ensure standardized and efficient coordination, Standard Operational Procedures are to be developed for each sector. The appointment of Security Liaison Officers is a critical requirement, and failure to comply with this provision is subject to penalties under Article 21 of the law.

This chapter underscores the law's focus on structured and comprehensive security planning and coordination, emphasizing the need for detailed security measures and robust communication channels between various stakeholders in the realm of critical infrastructure protection.

CHAPTER IV

Chapter IV of Law No. 06/L –014 focuses on European Critical Infrastructure (ECI) and encompasses the processes for identification, designation, and management of ECIs.

The chapter defines ECI as critical infrastructure within any European country that, if disrupted, would significantly impact at least two other European countries. The Government of Kosovo, through the Ministry of Internal Affairs (MIA), is tasked with identifying potential ECIs, particularly in energy and transport sectors. In doing so, the Government may consult with the European Commission. The identification process involves satisfying both cross-cutting and sectoral criteria and adhering to specific definitions outlined in the law.

Once a potential ECI is identified within Kosovo, MIA engages in discussions with affected European countries to designate it formally as an ECI. Information regarding potential ECI designation is classified according to domestic legislation. Additionally, if a critical infrastructure in another European country is deemed significant to Kosovo, the Government may propose it to be designated as an ECI.

The law also specifies that Operator Security Plans (OSPs) for ECIs are subject to the same regulations as national critical infrastructures and must be reviewed annually. Moreover, each ECI must appoint a Security Liaison Officer within 15 days of its designation. This officer is crucial for facilitating communication between the infrastructure's management and MIA. Failure to comply with this requirement is punishable.

In terms of reporting, the Government is required to conduct threat assessments for ECI subsectors and report every two years to the European Commission on various risks and vulnerabilities associated with each ECI sector. This process assists in assessing the need for additional protection measures at the European Community level.

Lastly, Chapter IV highlights the handling of sensitive ECI information. Individuals dealing with this information must possess appropriate security vetting, and the provisions also apply to non-written information exchanged during meetings. MIA serves as the Contact Point for ECI Protection, ensuring effective communication and coordination with European countries and the European Commission. This chapter emphasizes the collaborative and security-focused approach necessary for managing ECIs that have a transnational impact within Europe.

CHAPTER V

Chapter V of Law No. 06/L –014 outlines the processes for monitoring, supervision, and evaluation of the critical infrastructure system in the Republic of Kosovo.

The Ministry of Internal Affairs (MIA) plays a crucial role in these processes. It is responsible for preparing annual reports on the types of risks, threats, and vulnerabilities encountered in each sector of National Critical Infrastructure. These reports are classified and are made available to the Parliamentary Committee responsible for internal affairs and security. MIA also has the authority to prepare reports on specific national critical infrastructures if deemed necessary or requested by the Prime Minister.

Supervision of the law's implementation is also a key responsibility of the MIA. This includes conducting inspections and initiating appropriate responses, such as infringement procedures, when violations are discovered.

Handling sensitive national information is a critical aspect covered in this chapter. Anyone dealing with classified information under this law is required to have an appropriate level of security vetting, and this applies to both written and non-written information.

Penalty measures for non-compliance with various aspects of the law are clearly defined. Fines are imposed for failures such as not developing an Operator Security Plan or not appointing a Security Liaison Officer, with different fine scales for owners/operators, individuals, and individual business owners.

Furthermore, the chapter mandates the MIA to issue sub-legal acts for the law's implementation within six months of its entry into force. Finally, the law stipulates that it will come into force one year after its publication in the Official Gazette of the Republic of Kosovo.

Overall, Chapter V emphasizes the importance of continuous monitoring and evaluation, strict supervision, and the enforcement of compliance through penalties, ensuring a robust framework for managing and safeguarding Kosovo's critical infrastructure.

ANNEX 1

Annex 1 of Law No. 06/L –014 categorizes critical infrastructure within the European context, focusing on the Energy and Transport sectors. These sectors are crucial to the functioning and stability of multiple European countries, and their disruption could have widespread and significant impacts.

In the Energy sector, the law recognizes the critical nature of infrastructure related to electricity, oil, and gas. This includes all components essential for the production, transmission, storage, and distribution of energy resources. The resilience and security of these infrastructures are vital for maintaining energy supplies and supporting economic stability across Europe.

The Transport sector is similarly critical, encompassing a broad range of infrastructures that facilitate movement and connectivity. This includes major road networks, rail systems, air transport facilities, inland waterways, and maritime transport infrastructures. These subsectors are integral to both national and international travel, trade, and logistics, underscoring the importance of their protection and efficient management.

Overall, Annex 1 provides a clear and

structured framework for identifying and prioritizing European Critical Infrastructures within the Energy and Transport sectors. This classification assists in focusing efforts on protecting infrastructures that are essential for the maintenance of vital societal functions and cross-border collaboration in the European region.

ANNEX 2

Annex 2 of Law No. 06/L –014 provides a detailed and structured procedure for identifying European Critical Infrastructures. This process is critical for ensuring that the most impactful and significant infrastructures across Europe are recognized and appropriately managed for their transnational importance.

The identification process begins with the application of sectoral criteria by the Ministry of Internal Affairs (MIA) to select critical infrastructures within a specific sector. Following this initial selection, the MIA applies the definition of national critical infrastructure, as specified in the law, to assess the significance of the impact of potential ECIs. This step involves evaluating the availability of alternatives and the expected duration of service disruption or recovery for infrastructures that provide essential services.

In the subsequent step, the MIA applies the transboundary element of the ECI definition to the potential infrastructures that have passed the initial stages. This includes considering the potential cross-border impact of infrastructure disruption and the availability of service alternatives.

The final step involves applying cross-cutting criteria, where the severity of the impact of potential ECIs is examined, along with factors such as service alternatives and recovery duration. Only those infrastructures that satisfy these rigorous criteria are considered as ECIs. Infrastructures that do not meet these criteria are excluded from being designated as ECIs.

This procedure ensures a detailed and thorough approach to identifying ECIs, focusing on the most critical aspects such as impact severity, service essentiality, and transboundary effects. It underscores the law's commitment to a systematic and comprehensive evaluation of infrastructures that are vital not only to individual nations but also to the broader European context.

OVERVIEW OF THE EU'S DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES (2022/2557)

The European Union's Directive 2022/2557 marks a crucial shift in the EU's strategy for ensuring the resilience of critical entities. This Directive, which **replaces the previous Council Directive 2008/114/EC,** refocuses efforts from solely protecting critical infrastructure to a broader objective of enhancing resilience. This evolution is in response to the increasingly interconnected nature of the EU's critical infrastructure and the need for a comprehensive approach that extends beyond protection to include resilience measures.

A central element of this Directive is its acknowledgment of the varied threats that critical entities face, ranging from hybrid and terrorist attacks to natural disasters and climate change impacts. These threats, along with the growing interdependencies between different infrastructure sectors, underscore the need for a dynamic and flexible response mechanism.

The Directive also emphasizes the importance of aligning its objectives with other EU initiatives, particularly EU Directive 2022/2555, known as EU NIS 2 Directive, which focuses on cybersecurity. This alignment ensures a coherent approach that addresses both cyber and non-cyber risks, reflecting the comprehensive nature of the threats faced by critical entities.

To realize these objectives, the Directive emphasizes the importance of Member States developing strategies and performing risk assessments. These steps are crucial for identifying critical entities and supporting them in enhancing their resilience. The Directive also discusses the role of competent authorities in supervising and enforcing compliance, ensuring that critical entities adhere to the resilience requirements.

A significant provision is outlined in Article 27, which **announces the repeal of Directive 2008/114/EC, effective from October 18, 2024**. This means that from this date, Directive 2008/114/EC will no longer be legally binding or enforceable. Consequently, any laws, regulations, or actions previously governed by this directive will become obsolete. This repeal signifies a transition to the new, more comprehensive framework established by Directive (EU) 2022/2557. This change is especially important for Kosovo, which, while not a member of the EU, seeks to align its legislation with EU standards. The Law on Critical Infrastructure in Kosovo is fully based on Directive 2008/114/EC, and its repeal necessitates a significant reassessment and potential restructuring of Kosovo's legal framework regarding critical infrastructure.

In summary, Directive (EU) 2022/2557 establishes a clear and compelling rationale for a unified EU approach to enhancing the resilience of critical entities. It lays the groundwork for a legislative framework that addresses current and future threats in a harmonized, comprehensive manner, recognizing the crucial role these entities play in the functioning of the EU's internal market.

The EU Directive 2022/2557 is structured into eight chapters.

CHAPTER I

Chapter I of Directive (EU) 2022/2557 lays a foundational framework for enhancing the resilience of critical entities within the European Union. . The initial section focuses on setting obligations and procedures for Member States and critical entities to ensure the uninterrupted provision of essential services. This includes implementing measures for identifying and supporting critical entities, setting rules for their supervision, and enforcing standards for resilience. The Directive recognizes the importance of coordinating these efforts with other EU regulations, particularly in the realms of cybersecurity and data protection.

The subsequent section provides clear definitions of key terms such as 'critical entity', 'resilience', and 'incident', which are crucial for understanding and implementing the Directive's objectives. These definitions establish a common language and understanding for Member States, facilitating uniform application across the EU.

Further, the chapter addresses the Directive's role as a tool for minimum harmonization. It allows Member States the flexibility to adopt or maintain national laws that aim for a higher level of resilience, provided these laws are in line with the Union's overall legal framework. This flexibility acknowledges the varied security needs and capabilities of individual Member States while maintaining a consistent and coordinated approach at the Union level.

Overall, Chapter I is crucial in setting the tone and direction for the EU's approach to securing critical entities. It highlights the importance of cooperation, transparency, and flexibility, aiming to guarantee the effective provision of essential services across Member States.

CHAPTER II

Chapter II of Directive (EU) 2022/2557 focuses on establishing national frameworks for the resilience of critical entities. The chapter outlines the responsibilities of Member States in developing comprehensive strategies to enhance the resilience of critical entities. These strategies are expected to be comprehensive, encompassing strategic objectives, governance frameworks, identification processes for critical entities, and measures for enhancing overall resilience.

Risk assessments are a key component, with Member States required to evaluate potential risks, including natural and man-made disasters, and their impact on critical entities. The outcomes of these risk assessments are essential for identifying critical entities, which are mandated to be completed by July 2026. The Directive provides specific criteria for determining the significance of disruptive effects on essential services.

The Directive also addresses the roles and responsibilities of competent authorities and single points of contact in each Member State. These entities are tasked with ensuring effective application, enforcement, and cross-border cooperation regarding the Directive's provisions. They also play a crucial role in information sharing and consultation among Member States, particularly in situations where critical entities have cross-border impacts or are part of multinational corporate structures.

Furthermore, the Directive encourages Member States to support critical entities through guidance, training, and potential financial resources to enhance their resilience. This includes facilitating information sharing and the exchange of

best practices among critical entities.

In summary, Chapter II presents a structured methodology for Member States to enhance the resilience of critical entities through comprehensive strategies, risk assessments, identification and designation processes, and cooperative frameworks both within and across Member State borders. This framework is crucial for maintaining the continuous delivery of essential services and protecting the societal and economic functions within the EU.

CHAPTER III

Chapter III of Directive (EU) 2022/2557 focuses on the resilience of critical entities within the European Union. It mandates that these entities conduct comprehensive risk assessments to evaluate potential disruptions to their essential services. These assessments must consider a broad range of risks, including natural disasters, public health emergencies, and other potential threats. They should also consider dependencies on various sectors and entities, including those in neighboring countries.

To ensure resilience, critical entities are required to implement various technical, security, and organizational measures. These measures include preventing incidents, securing physical infrastructure, effectively responding to and recovering from incidents, managing employee security, and raising awareness among personnel. Entities are also required to maintain a resilience plan detailing these measures and designate a liaison officer for communication with competent authorities.

One key section specifies conditions under which **critical entities can conduct background checks on individuals in sensitive roles or with access to critical systems**, ensuring these checks are consistent with EU and national laws.

Regarding incident response, the chapter requires critical entities to promptly notify competent authorities about incidents that significantly disrupt essential services. This notification should include details that help understand the incident's nature, cause, and potential consequences. For incidents with significant cross-border impacts, a wider notification mechanism is activated.

Furthermore, the chapter promotes the use of European and international standards to ensure a harmonized approach to implementing security and resilience measures across critical entities.

Overall, Chapter III establishes a robust framework for critical entities to assess risks, implement resilience measures, conduct necessary background checks, and ensure timely incident notification, all within a standardized approach guided by European and international standards. This framework is crucial for maintaining the integrity and continuity of essential services provided by critical entities across the European Union.

CHAPTER IV

Chapter IV of Directive (EU) 2022/2557 introduces the concept of critical entities of particular European significance and outlines a framework for their identification and assessment. This category includes entities that offer essential services across six or more Member States and are already recognized as critical entities in a previous section of the Directive. These entities are obliged to inform their respective competent

authorities, who then communicate this information to the European Commission.

A key feature of this chapter is the organization of advisory missions by the Commission. These missions are designed to evaluate the measures implemented by these entities to comply with their obligations under Chapter III, focusing on resilience. The initiation of these missions can be at the request of Member States or the Commission's initiative. During these missions, Member States are required to provide relevant information, including risk assessments and measures taken to ensure resilience.

The advisory missions include experts from the Member States involved and Commission representatives. They are responsible for reporting their findings, which are then analyzed to assess the entity's compliance with required obligations and to suggest improvements in resilience measures.

The Commission is tasked with setting procedural rules for these missions through implementing acts, ensuring that they are conducted efficiently and effectively. Critical entities of particular European significance are obliged to grant these missions access to necessary information and facilities. The findings from these missions, along with lessons learned, are shared with the Critical Entities Resilience Group, promoting mutual learning and enhancing resilience across the EU.

In summary, Chapter IV establishes a collaborative and evaluative process involving the Commission and Member States. This mechanism ensures that critical entities of European significance meet the highest standards of resilience. This process emphasizes the importance of these entities in maintaining the continuity and security of essential services across multiple Member States.

CHAPTER V

Chapter V of Directive (EU) 2022/2557 details the establishment and functioning of the Critical Entities Resilience Group and outlines the support role of the European Commission.

The Critical Entities Resilience Group is a key component in this framework, created to support the Commission and facilitate cooperation among Member States. It serves as a platform for exchanging information related to the Directive, including strategies, best practices, risk assessments, and incident notifications. The Group is comprised of representatives from the Member States and the Commission, with potential involvement from other stakeholders and experts. One of its primary roles is to analyze strategies and reports to identify best practices and promote shared learning among Member States. The Group will establish a biennial work programme and hold regular meetings, including with the Cooperation Group under Directive (EU) 2022/2555, to ensure aligned and effective cooperation.

The European Commission plays a supportive role, assisting Member States and critical entities in fulfilling their obligations under the Directive. This includes preparing overviews of cross-border and cross-sectoral risks, organizing advisory missions, and facilitating the exchange of information and expertise across the EU. Additionally, the Commission will develop best practices, guidance materials, and methodologies to complement the activities of Member States in enhancing the resilience of critical entities. This role also extends to informing Member States about available EU financial resources that can be leveraged to strengthen resilience.

In principle, Chapter V establishes a collaborative ecosystem involving the Critical Entities Resilience Group and the European Commission, aimed at enhancing the resilience of critical entities across the EU. This collaborative approach is crucial for addressing the complex and interconnected challenges faced by critical entities, ensuring a coordinated and effective response to enhance the security and continuity of essential services.

CHAPTER VI

Chapter VI of Directive (EU) 2022/2557 addresses the supervision and enforcement mechanisms to ensure compliance with the Directive, focusing on the role of competent authorities and the establishment of penalties for non-compliance.

This chapter of the Directive empowers competent authorities in Member States to conduct thorough assessments of critical entities' compliance. These assessments can include on-site inspections of infrastructure and premises, off-site supervision, and mandatory audits. Critical entities are required to provide necessary information and evidence, such as the results of independent audits, to demonstrate their resilience measures. If non-compliance is identified, competent authorities have the authority to issue orders for corrective actions within set deadlines. The Directive emphasizes that these supervisory powers must be executed with appropriate safeguards to guarantee fairness, transparency, and proportionality, and to protect the rights and interests of the entities.

Moreover, the chapter sets up a framework for cooperation and information exchange between the competent authorities under this Directive and those under Directive (EU) 2022/2555 known as EU NIS 2 Directive, reflecting the interconnected nature of physical and cybersecurity aspects of critical entities.

Furthermore, the chapter obliges Member States to define and implement penalties for violations of the national measures adopted under this Directive. These penalties must be effective, proportionate, and dissuasive, ensuring that they effectively deter non-compliance. Member States are required to inform the Commission of their penalty rules and any subsequent modifications.

Overall, Chapter VI creates a robust supervision and enforcement framework, ensuring that critical entities comply with the Directive's requirements. The collaborative approach between different supervisory bodies and the focus on proportionate penalties reinforce the Directive's aim to enhance the resilience of critical entities throughout the European Union.

CHAPTER VII

Chapter VII of Directive (EU) 2022/2557 outlines the procedures related to the adoption of delegated and implementing acts by the European Commission. This chapter establishes the legal and procedural framework for the Commission to exercise its powers in refining and implementing the Directive.

The chapter details the process for the Commission to adopt delegated acts. This includes the conditions under which these powers are granted, including the time frame for their exercise (**five years from January 16, 2023**), and the mechanism for their potential revocation by the European Parliament or the Council. Importantly, it

mandates that the Commission consult with experts from each Member State prior to adopting any delegated act, ensuring that the perspectives and expertise of all Member States are considered. It also specifies the process for notification of the adopted acts to the European Parliament and the Council, along with the requirement for these bodies to either express objection or consent within a specified period, thus offering a check on the Commission's delegated powers.

This chapter also describes the committee procedure, stating that the Commission will be assisted by a committee as defined in Regulation (EU) No 182/2011. This regulation outlines the framework for committees that control the exercise of implementing powers by the Commission, thereby ensuring oversight and involvement of Member States in the implementation process of the Directive.

Overall, Chapter VII ensures that the adoption of delegated and implementing acts by the Commission occurs within a structured and transparent framework, involving consultation with Member State experts and oversight by the European Parliament and the Council. This process aims to ensure that the Directive's implementation is both effective and reflective of the collective interests and expertise of the EU Member States.

CHAPTER VIII

Chapter VIII of Directive (EU) 2022/2557 contains the final provisions concerning reporting, review, transposition, repeal, entry into force, and the addressees of the Directive.

This chapter includes a mandate for the European Commission to evaluate and report on each Member State's compliance with the Directive by **July 17, 2027**. The Commission is also tasked with conducting regular reviews of the Directive's effectiveness. These reviews are intended to assess the Directive's impact on the resilience of critical entities and determine if any modifications are necessary. The first of these reviews is scheduled for **June 17, 2029**, and will incorporate feedback from the Critical Entities Resilience Group.

The chapter also specifies the transposition requirements for Member States, setting a deadline of **October 17, 2024**, for adopting the necessary measures to comply with the Directive, with these measures coming into effect the following day. Additionally, it requires Member States to reference this Directive when they publish their national measures.

Furthermore, the chapter announces the repeal of Directive 2008/114/EC effective from **October 18, 2024**, and clarifies that references to the repealed Directive should be understood as references to the new Directive.

The chapter also indicates that the Directive will come into force twenty days following its publication in the Official Journal of the European Union.

Finally, it specifies that the Directive is addressed to the Member States, highlighting its applicability and relevance to them.

In summary, Chapter VIII provides the framework for the implementation, assessment, and continuous review of the Directive, ensuring that its objectives are effectively integrated into national laws and practices of the Member States, and that its efficacy in enhancing the resilience of critical entities is regularly evaluated.

OVERVIEW OF THE EU'S NIS 2 DIRECTIVE

EU Directive 2022/2555, also known as **EU NIS 2 Directive**, enacted on December 14, 2022, aims to achieve a high common level of cybersecurity across the European Union. It modifies Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repeals Directive (EU) 2016/1148 (NIS 1 Directive).

The predecessor, Directive (EU) 2016/1148 (NIS 1 Directive), was important in developing the EU's cybersecurity capabilities and cooperation. However, evolving cybersecurity challenges necessitated this new directive. The new EU NIS 2 Directive acknowledges the growing complexity of network and information systems, the expanding cyber threat landscape, and the increasing frequency and impact of cyber incidents.

The directive extends its scope to a broader range of sectors, recognizing the obsolete differentiation between operators of essential services and digital service providers. It establishes a uniform criterion to identify entities falling within its scope, primarily based on size (medium-sized enterprises and above). Certain entities, like those predominantly involved in national security or law enforcement, are excluded from its scope.

Entities are classified into two categories: **essential** and **important**, with compliance obligations tailored to their criticality and size. The directive mandates comprehensive cybersecurity risk management and incident reporting for these entities. It emphasizes the need for entities to manage supply chain risks and adopt cyber hygiene practices.

Enhanced cooperation is encouraged at the EU level, including information sharing about cyber threats and vulnerabilities. The directive supports the development of voluntary cybersecurity information-sharing arrangements and the establishment of a European vulnerability database by ENISA.

The directive aims to remove divergences among Member States in cybersecurity standards, thereby reducing market fragmentation and enhancing resilience against cyber threats. Member States are required to transpose the directive into national law, ensuring alignment with its provisions.

Compliance with EU data protection laws is emphasized, ensuring respect for privacy and personal data protection. The directive is aligned with fundamental rights as recognized in the EU Charter and the European Commission is tasked with periodic reviews to propose amendments in response to technological, societal, or market changes.

The EU NIS 2 Directive represents a significant step towards harmonizing and elevating cybersecurity standards across the European Union, addressing emerging challenges and enhancing overall digital security and resilience.

The Directive is structured into nine chapters and two annexes.

CHAPTER I

Chapter I of the Directive (EU) 2022/2555 sets the foundation for a unified and high-standard cybersecurity framework across the European Union. It aims to enhance the functioning of the internal market by imposing structured cybersecurity measures. The Directive applies to a broad range of entities, including public and private sectors, specifically targeting medium-sized and larger enterprises. It also covers entities providing critical services, regardless of their size, in domains like electronic communications, trust services, and domain name systems.

The Directive mandates Member States to adopt national cybersecurity strategies and designate relevant authorities and response teams. It requires entities to adhere to specific risk management practices and report significant cybersecurity incidents. Additionally, the Directive promotes cybersecurity information sharing and establishes supervisory and enforcement responsibilities for Member States.

A key aspect of the Directive is its flexibility and integration with sector-specific Union legal acts, allowing for harmonized application across different sectors. It sets minimum harmonization standards, allowing Member States to adopt more stringent measures if desired.

The definitions in this chapter are comprehensive, covering a wide range of terms essential for the uniform interpretation and implementation of the Directive across the EU. This chapter effectively lays the groundwork for a coordinated and robust approach to cybersecurity, emphasizing cooperation, information sharing, and consistent application of cybersecurity practices across Member States.

CHAPTER II

Chapter II of Directive (EU) 2022/2555 establishes a coordinated cybersecurity framework, emphasizing the need for Member States to adopt comprehensive national cybersecurity strategies. These strategies should focus on identifying risks, preparing for incidents, and fostering collaboration between public and private sectors.

The chapter mandates the designation of competent authorities and single points of contact for cybersecurity, ensuring adequate resources for effective implementation of the Directive. These entities are responsible for monitoring Directive implementation, liaising for cross-border cooperation, and facilitating efficient cybersecurity operations at the national level.

The development of national cyber crisis management frameworks is another critical aspect, requiring Member States to designate authorities for managing large-scale cybersecurity incidents. Each Member State must also establish a detailed response plan for such incidents, integrating cyber crisis management into the broader national crisis management framework.

The establishment of CSIRTs is crucial for handling security incidents. These teams are tasked with monitoring and analyzing cyber threats, providing early warnings, and responding to incidents. The Directive also emphasizes the importance of secure communication infrastructures for CSIRTs and encourages international cooperation and information exchange.

An innovative component of the chapter is the introduction of a coordinated vulnerability disclosure process, with a designated CSIRT acting as a coordinator. Additionally, ENISA

is tasked with developing and maintaining a European vulnerability database, facilitating the reporting and management of vulnerabilities.

Finally, the chapter underscores the importance of cooperation at the national level among various authorities, ensuring effective communication and information sharing. This cooperation is vital for a unified approach to cybersecurity, aligning national strategies with the overarching goals of the Directive.

CHAPTER III

Chapter III focuses on strengthening cooperation at both the Union and international levels to enhance cybersecurity. This includes establishing structures for strategic cooperation, operational coordination, and sharing best practices among Member States.

The Cooperation Group, composed of representatives from Member States, the Commission, and ENISA, plays a pivotal role in guiding the Directive's implementation and facilitating information exchange on cybersecurity matters. This group operates on biennial work programs, exchanging expertise and insights on various aspects of cybersecurity.

The CSIRTs network, comprising representatives of national CSIRTs, focuses on operational cooperation. It facilitates the sharing of technology, information on cyber threats and incidents, and the development of coordinated responses to cybersecurity challenges.

EU-CyCLONe, another key component, is dedicated to managing large-scale cybersecurity incidents and crises at the operational level. It aims to develop a shared situational awareness and coordinate management strategies during such events.

International cooperation is also emphasized, with provisions for the Union to engage with third countries or international organizations in cybersecurity activities. This fosters a global approach to addressing cyber threats.

ENISA's role includes developing a biennial report on the state of cybersecurity in the Union, assessing risks, capabilities, awareness levels, and providing policy recommendations. This report is crucial for understanding and addressing the evolving cybersecurity landscape.

Finally, the chapter introduces the concept of peer reviews, a voluntary process where Member States assess each other's cybersecurity capabilities and implementation of the Directive. These reviews, conducted by designated cybersecurity experts, provide valuable insights and recommendations for improving cybersecurity practices across the Union.

Overall, Chapter III establishes a robust framework for cooperation and information exchange at various levels, essential for a cohesive and effective response to cybersecurity challenges in the Union and beyond.

CHAPTER IV

Chapter IV outlines the requirements for cybersecurity risk management and reporting obligations for essential and important entities. The chapter emphasizes the responsibility of management bodies in overseeing and implementing cybersecurity measures and mandates regular training for both management and employees.

Entities are required to adopt comprehensive cybersecurity measures based on an all-hazards approach, including policies for risk analysis, incident handling, and business continuity. These measures must be appropriate to the level of risk and the size of the entity, and entities are obligated to take corrective actions if they do not comply.

A significant focus of this chapter is on the reporting of cybersecurity incidents. Entities are required to promptly notify relevant authorities of significant incidents and communicate potential cyber threats to service recipients. The chapter also allows for public disclosure of significant incidents in certain circumstances.

Additionally, the chapter introduces the use of European cybersecurity certification schemes. Member States may require entities to use certified ICT products, services, and processes, and the Commission has the authority to specify which categories of entities should use these certified solutions.

Finally, the chapter promotes the use of European and international standards in cybersecurity, with ENISA providing guidance on relevant technical areas and existing standards.

Overall, Chapter IV establishes a robust framework for managing and reporting cybersecurity risks, emphasizing the importance of proactive measures, effective communication, and compliance with standards to enhance cybersecurity across essential and important entities.

CHAPTER V

Chapter V of the Directive outlines jurisdiction, territoriality, and registration guidelines for various entities covered by the Directive.

This chapter specifies that entities are generally subject to the jurisdiction of the Member State where they are established. However, specific rules apply to different types of entities, including those not established in the EU but offering services within it. These entities must designate a representative in the EU, although this does not protect the entity from legal actions.

A significant aspect of this chapter is the mandate for the European Union Agency for Cybersecurity (ENISA) to establish a comprehensive registry of service providers. Entities are required to submit and regularly update their information to competent authorities, which is then forwarded to ENISA.

Further, the chapter focuses on the collection and maintenance of accurate domain name registration data. Top-Level Domain (TLD) name registries and domain name registration services are required to have verification policies to ensure data accuracy. Non-personal registration data must be publicly available, and access to specific data should be provided upon lawful requests. Additionally, it emphasizes the need to avoid duplication in data collection.

Overall, Chapter V establishes clear rules for determining the jurisdiction of entities under the Directive and requires the maintenance of registries and databases to ensure accountability and transparency in domain name registration and service provision.

CHAPTER VI

Chapter VI of the Directive focuses on information sharing related to cybersecurity, providing guidelines for voluntary exchange and notification.

This chapter introduces a framework for the voluntary sharing of cybersecurity-

related information. This exchange includes a wide range of cybersecurity information aimed at enhancing overall cybersecurity levels and response capabilities. The EU Member States play a role in facilitating the establishment of these information-sharing arrangements, ensuring sensitive information is handled appropriately. Entities are required to inform competent authorities about their participation in these arrangements.

Further, the chapter extends the scope of information sharing, allowing both essential and important entities, and other entities, to voluntarily report incidents, threats, and near misses to the CSIRTs or competent authorities. The processing of these voluntary notifications is managed similarly to mandatory notifications, with a possibility for prioritization. Importantly, voluntary reporting does not subject the entity to any additional obligations beyond those that would exist without the notification. The confidentiality and appropriate protection of the information provided by the notifying entity are emphasized.

In summary, Chapter VI encourages a collaborative approach to cybersecurity, promoting the sharing of vital information among various entities to enhance preparedness and response to cyber threats and incidents. This cooperation is facilitated by Member States and managed to ensure the protection and appropriate use of shared information.

CHAPTER VII

Chapter VII of the Directive focuses on the supervision and enforcement mechanisms to ensure compliance.

This chapter presents the overall framework for supervision and enforcement, emphasizing the need for effective supervision, prioritization of tasks based on risk, and cooperation with data protection authorities. It also addresses the supervision of public administration entities, ensuring operational independence for competent authorities.

The chapter further elaborates on the supervisory and enforcement measures for essential entities. This includes a range of powers for competent authorities, from on-site inspections to security audits, and the authority to issue binding instructions and impose fines. It also holds the management of these entities responsible for compliance.

Additionally, the chapter extends similar provisions to important entities, with a particular focus on supervisory measures after the fact.

There are guidelines for imposing administrative fines on essential and important entities, with maximum limits based on either a percentage of total worldwide annual turnover or fixed amounts.

The chapter also emphasizes the necessity of cooperation with data protection authorities in instances of personal data breaches, ensuring alignment with the General Data Protection Regulation (GDPR). Member States are mandated to establish national rules for penalties relevant to infringements of this Directive.

Lastly, the chapter encourages mutual assistance and cooperation among competent authorities across Member States, particularly in cross-border scenarios. It sets out the framework for such cooperation, including joint supervisory actions and the sharing of information and resources.

In summary, Chapter VII establishes a comprehensive framework for supervising and enforcing compliance with the Directive, providing competent authorities with the necessary powers and responsibilities. It emphasizes a coordinated approach, both within Member States and across borders, to effectively address cybersecurity challenges.

CHAPTER VIII

Chapter VIII of the Directive focuses on the delegation and implementation of acts, particularly the role of the European Commission and the procedures for adopting these acts.

This chapter addresses the delegation of power to the Commission, specifically for adopting delegated acts. This delegation is subject to certain conditions and a predefined timeline of five years from January 2023. The article also outlines the revocation process of this power by the European Parliament or Council. Before adopting a delegated act, the Commission is required to consult experts from each Member State. After adoption, the act is notified to the European Parliament and the Council and will only enter into force if no objection is raised within a specific period.

Additionally, the chapter details the committee procedure to support the Commission. This committee operates under the framework of Regulation (EU) No 182/2011. The article explains the application of this regulation, particularly regarding the procedure for obtaining committee opinions. It also states the conditions under which a written procedure can be terminated.

In summary, Chapter VIII provides the legal framework for the Commission's role in adopting delegated acts and outlines the procedural requirements for the committee assisting the Commission in this task. It emphasizes the importance of consultation, notification, and the option for the European Parliament and Council to object to the Commission's acts, ensuring checks and balances in the legislative process.

CHAPTER IX

Chapter IX of the Directive outlines the final provisions, focusing on the review process, transposition, amendments to existing legislation, repeal of previous directives, the effective date, and addressees of the Directive.

This chapter introduces a periodic review schedule for the Commission to assess the Directive's effectiveness and impact, particularly in relation to the economy and society's cybersecurity needs. It also mentions the potential for legislative proposals based on these reviews.

The chapter sets a deadline for Member States to adopt necessary measures to comply with the Directive and mandates that these measures reference this Directive upon their official publication.

Further, the chapter specifies amendments to existing EU regulations and directives, particularly the deletion of certain articles from Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, effective from 18 October 2024.

Additionally, the chapter announces **the repeal of Directive (EU) 2016/1148 known as EU NIS 1 Directive, effective from 18 October 2024**, and clarifies how references to the repealed directive should be interpreted.

The chapter also declares the Directive's entry into force, which occurs twenty days following its publication in the Official Journal of the European Union.

Lastly, the chapter identifies the Directive's addressees, which are the Member States of the European Union.

In principle, Chapter IX provides the legal and procedural framework for the Directive's implementation, amendment of existing laws, periodic review and assessment, and its applicational scope within the EU Member States.

ANNEX I

Annex I outlines the critical sectors and subsectors, with specific types of entities under each category, that are subject to the Directive's provisions. This classification serves to identify key areas of focus for cybersecurity measures and compliance, spanning diverse fields such as energy, transport, banking, health, digital infrastructure, and public administration. The Annex ensures that entities across these essential sectors are adequately protected and regulated, given their significance to national and economic security.

ANNEX II

Annex II identifies other sectors considered critical for cybersecurity provisions, expanding the scope beyond the primary sectors in Annex I. It includes sectors like postal and courier services, waste management, chemical manufacture and distribution, food production and distribution, various manufacturing subsectors, digital service providers, and research organizations. This classification aims to encompass a broader range of entities that, while not as critical as those in Annex I, still play significant roles in maintaining societal and economic stability and security. The inclusion of these sectors ensures a comprehensive approach to cybersecurity, safeguarding a wider spectrum of essential services and infrastructure.

COMPARATIVE ANALYSIS

1. Law on Critical Infrastructure vs EU Directive 2022/2555 on the Resilience of Critical Entities

In the scope of critical infrastructure, distinct approaches are evident between Law No. 06/L –014 on Critical Infrastructure in Kosovo and the Directive (EU) 2022/2557 on the Resilience of Critical Entities.

Law No. 06/L –014 on Critical Infrastructure in Kosovo, established by Decree No. DL-016-2018, was initially promulgated with an aim to align with the European Union standards, drawing its foundation from the then-prevailing EU Directive 2008/114/EC of 8 December 2008. This law was a crucial step for Kosovo, showing its commitment to safeguarding national and European critical infrastructures, in that way ensuring the welfare and stability of its citizens. It structured a comprehensive legal framework focusing primarily on the energy and transport sectors, encompassing risk analysis, security coordination, and reporting mechanisms, mirroring the directives of the EU legislation of that time.

However, the landscape of critical infrastructure management has evolved significantly since then. The EU Directive 2008/114/EC, which served as a cornerstone for Kosovo's law, has been repealed and replaced by the new Directive (EU) 2022/2557. This replacement marks a significant shift in the EU's approach towards critical infrastructure – from a protection-based paradigm to a resilience-oriented framework. The new Directive broadens the scope beyond traditional sectors and emphasizes addressing a wider spectrum of threats, including hybrid, terrorist, and climate change-related risks. It advocates for comprehensive risk assessments, integrating dependencies across various sectors and countries, and underscores the importance of resilience planning, cross-border cooperation, and efficient information sharing.

This evolution in EU policy renders an urgent need for Kosovo to revisit and revise its Law on Critical Infrastructure. While Law No. 06/L –014 was comprehensive and aligned with EU standards at the time of its enactment, aligning it with the new Directive (EU) 2022/2557 has become essential to ensure its relevance and efficacy in the current context. The new Directive's emphasis on resilience, broader risk assessments, and cooperative mechanisms for critical entities presents an opportunity for Kosovo to enhance its infrastructure protection strategies and harmonize with the updated EU standards.

In terms of risk assessment and management, the Kosovo Law establishes a process for risk analysis aimed at identifying and designating critical infrastructures, coupled with the requirement for the development of Operator Security Plans (OSPs). These OSPs are pivotal in ensuring that designated infrastructures have robust security measures in place. In contrast, the EU Directive advocates for more comprehensive risk assessments from critical entities. It recognizes the wide array of risks and dependencies that extend beyond national boundaries and sectoral confines, urging a holistic view of risk management.

The aspect of security planning and coordination also highlights differences. The Kosovo Law focuses on sector-specific protection and coordination, establishing roles that are pivotal for the management of security within individual sectors. Conversely, the EU Directive calls for an array of technical, security, and organizational measures, mandating the maintenance of resilience plans. It goes a step further by requiring liaison officers for effective communication with authorities, emphasizing the need for proactive and continuous engagement.

When it comes to reporting and information sharing, the Kosovo Law mandates strict reporting and information handling, especially for European Critical Infrastructures. This approach aims at maintaining a high level of information accuracy and security. In comparison, the EU Directive places significant emphasis on the sharing of information and cooperation among Member States. This focus, particularly for entities with cross-border impacts, underscores the importance of collaborative efforts in the face of shared risks.

The roles of monitoring and supervision are also distinctively addressed. The Kosovo Law assigns the Ministry of Internal Affairs a central role in monitoring, supervision, and evaluation, including the preparation of annual risk reports. This centralization reflects a focused approach to oversight. The EU Directive, in contrast, empowers competent authorities to supervise and enforce compliance, establishing a framework that includes penalties for non-compliance. This system signifies a more distributed approach to ensuring adherence to resilience and security standards.

For Kosovo, this means expanding the law's scope to include more sectors, adopting an integrated risk management approach, strengthening coordination mechanisms, developing robust reporting and information sharing systems, aligning monitoring and supervisory mechanisms with EU standards, and focusing on technological innovation. Such amendments will not only elevate Kosovo's infrastructure resilience but also fortify its alignment with the broader European framework for critical infrastructure protection.

In summary, while the Kosovo Law provides a solid foundation for the protection and management of critical infrastructures, focusing on specific sectors and structured roles, the EU Directive introduces a more expansive and integrated perspective. It emphasizes resilience, comprehensive risk assessments, diverse security measures, and EU-wide cooperation. For Kosovo, aligning its law with the EU Directive would mean embracing a broader scope of critical infrastructure management, a holistic approach to risk assessment, and an enhanced focus on cross-border cooperation and information sharing. This alignment would not only enhance Kosovo's infrastructure resilience but also integrate it more seamlessly into the broader European context of critical infrastructure protection.

2. Law on Critical Infrastructure vs EU NIS Directive 2022/2555

The Law on Critical Infrastructure in Kosovo represents a foundational effort by Kosovo to protect and manage its critical infrastructure, aligning with the European Union standards of that time. Designed to ensure the security and welfare of its citizens, this law focuses on vital sectors like energy and transport and establishes mechanisms for their oversight and protection. Key elements include the roles of Security Coordinators and Security Liaison Officers, and the requirement for developing Operator Security Plans (OSPs).

However, with the introduction of the 'Directive (EU) 2022/2555', there's a clear need to update the Kosovo Law to reflect the latest standards in critical infrastructure

management. This Directive marks a significant shift in the EU's approach, expanding the scope beyond traditional sectors to encompass a more diverse range of fields including healthcare, digital infrastructure, and public administration. It emphasizes a high level of cybersecurity across the EU, with a focus on risk management, incident reporting, and cooperation.

To bring the Kosovo Law in line with the Directive, several amendments are necessary:

1. **Expanding Sector Coverage:** The Kosovo Law should broaden its focus to include the additional sectors identified in the Directive. This change will ensure a more comprehensive approach to protecting all critical infrastructure sectors.

2. **Integrating Risk Management:** The law should adopt a more holistic approach to risk management, mirroring the Directive's emphasis on comprehensive risk assessment and mitigation strategies.

3. **Enhancing Security Planning and Coordination:** Provisions in the Kosovo Law regarding security planning, information sharing, and reporting need to be updated. This would involve setting up mechanisms for efficient information exchange and collaborative response to threats.

4. **Strengthening Monitoring and Supervision:** The law should enhance its monitoring and supervisory mechanisms to ensure effective compliance and enforcement, in line with EU standards.

5. **Adopting Technological Advancements:** Incorporating provisions for the adoption of advanced cybersecurity technologies and practices is crucial. This step would align Kosovo's approach with the European cybersecurity certification schemes endorsed by the Directive.

By implementing these updates, the Law on Critical Infrastructure in Kosovo will not only align with the latest EU standards but also strengthen its infrastructure resilience. This process is essential for Kosovo to effectively manage and protect its critical infrastructures in an increasingly interconnected and digitalized world, ensuring the safety and well-being of its citizens.

RECOMMENDATIONS

In the context of updating Kosovo's Law No. 06/L –014 on Critical Infrastructure, it's imperative to align with the evolving standards set by the EU, particularly in the wake of the new Directive (EU) 2022/2557 and the EU NIS 2 Directive 2022/2555. This requires not only a broadening of the law's scope but also a refinement of its focus to ensure comprehensive and modernized protection of critical infrastructure.

1. **Update to Align with New EU Directives:** The urgent revision of Law No. 06/L –014 is necessary to comply with the new Directive (EU) 2022/2557. This entails a paradigm shift from protection to resilience, accommodating an expanded array of threats and fostering a more interconnected approach to infrastructure management.

2. **Refinement of Sectoral Coverage:** Amend Article 5 to remove the concept of "2.8. national values" from the Sectors of Critical Infrastructure. This change will clarify and streamline the focus of the law, ensuring it is directly aligned with current priorities and threats.

3. **Inclusion of Diverse and Expanded Sectors:** Introduce a comprehensive list of sectors that reflect current critical infrastructure needs. These should be categorized into two groups:

SECTORS OF HIGH CRITICALITY:

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT service management (business-to-business)
- Public administration
- Space

OTHER CRITICAL SECTORS:

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Production, processing, and distribution of food
- Manufacturing
- Digital providers
- Research

4. **Holistic Risk Management:** Embed a comprehensive approach to risk assessment and management, considering the interdependencies across these sectors and the potential transnational impacts of threats.

5. **Enhanced Security and Resilience Planning:** Revise the law to include improved planning, coordination, and information-sharing mechanisms. This will facilitate a more collaborative and effective response to infrastructure threats and disruptions.

6. **Robust Monitoring and Supervisory Mechanisms:** Strengthen the supervisory roles, delineating clear mechanisms for compliance and enforcement to ensure adherence to the updated law's standards.

7. **Integration of Advanced Cybersecurity Technologies:** Adopt provisions for the use of cutting-edge cybersecurity technologies and practices. This should be in line with European cybersecurity standards and certification schemes.

8. **Promotion of International Cooperation:** Foster stronger international ties for knowledge exchange and collective efforts in critical infrastructure protection, particularly with EU Member States and relevant international organizations.

9. **Regular Review and Dynamic Adaptation:** Establish a system for the continuous review and adaptation of the law, making it responsive to technological advancements and emerging threat landscapes.

By implementing these recommendations, Kosovo will significantly enhance the resilience and security of its critical infrastructure. Such an update will ensure that the law is not only comprehensive and contemporary but also synchronized with the latest EU standards. This alignment is crucial for safeguarding Kosovo's infrastructure, thereby ensuring the safety and well-being of its citizens in a rapidly evolving global context.

ENDNOTES

1. Law No. 06/L-014 on Critical Infrastructure in Kosovo: https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
2. EUR-Lex: Council of the European Union - Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: https://eur-lex.europa.eu/eli/dir/2022/2557/oj
3. EUR-Lex: Council of the European Union - Directive 2022/2557 on the resilience of critical entities (CER Directive): https://eur-lex.europa.eu/eli/dir/2022/2557/oj
4. EUR-Lex: Council of the European Union - Directive 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive): https://eur-lex.europa.eu/eli/dir/2022/2555
5. EUR-Lex: Council of the European Union - Directive 2016/1148 on measures for a high common level of security of network and information systems across the Union (NIS 1 Directive): https://eur-lex.europa.eu/eli/dir/2016/1148/oj
6. European Commission - Critical Infrastructure Resilience: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en
7. European Commission - CER and NIS-2 Directives: https://ec.europa.eu/newsroom/cipr/items/764849/en
8. European Commission - Register of Commission Expert Groups and Other Similar Entities: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3889
9. ENISA – NIS 2 Directive: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
10. ENISA – EU CyCLONe: https://www.enisa.europa.eu/topics/incident-response/cyclone
11. European Parliament – The NIS 2 Directive: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
12. QKSS - Enhancing Critical Infrastructure Identification in Kosovo: https://qkss.org/images/uploads/files/Critsica_infrastructue_2023_1.pdf

Katalogimi në botim – **(CIP)**

Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

34:338.49(495.51)(047)

341.176(4)

Limaj, Besnik

Aligning Kosovo's critical infrastructure law with the EU's directive on the resilience of critical entities and EU's nis2 directive : a comparative study / Besnik Limaj. - Prishtinë : QKSS, 2024. - 32 f. ; 24 cm.

ISBN 978-9951-842-18-1

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 978-9951-842-18-1