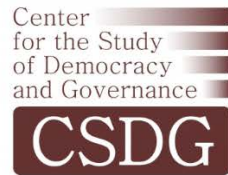




CYBER GOVERNANCE CHALLENGES FOR ALBANIA

—
ADDRESSING POLICY
CHOICE DILEMMAS





Kingdom of the Netherlands

Cyber Governance Challenges for Albania: Addressing policy choice dilemmas

Author:

Ilvana DEDJA

Internal review:

Arjan DYRMISHI

External Review:

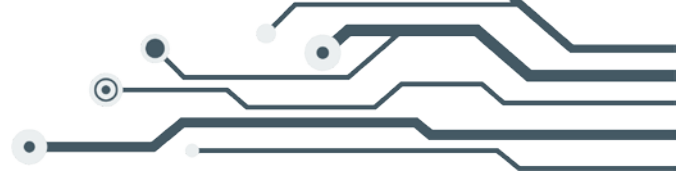
Jorgo ÇIPA

Design and layout

Ergys TEMALI

Images

Freepik.com



© September 2023, Center for the Study of Democracy and Governance (CSDG)

Acknowledgments

This policy paper is produced by the Center for the Study of Democracy and Governance in the framework of the project “Improved Policy Debate and Accountability to Delivering on Fundamentals First, through the Establishment of Cluster One EU Negotiations Platform – Albania (C1-EU-NPA)” with the support of the Netherlands Embassy in Tirana.

Disclaimer

The opinions, findings and recommendations expressed in this publication are those of the author and do not necessarily reflect the opinions or views of the Netherlands Embassy in Tirana.



TABLE OF CONTENTS

List of abbreviations	5
Executive Summary.....	6
Main findings and recommendations.....	11
Introduction	17
A brief cyber assessment of Albania.....	20
The EU cyber landscape	32
Pillar 1: Cybersecurity Strategy and Governance.....	35
Pillar 2: Investment and Research.....	42
Pillar 3: Policy Guidance and Coordination	44
Pillar 4: Cooperation and Diplomacy	48
Albania’s cyber landscape.....	49
Legal framework	51
Cybersecurity strategy.....	60
Cyber resilience and critical infrastructure protection.....	64
National cybersecurity governance	70
The dilemma	79
Scenario 1: Lagging in Cybersecurity advancement.....	80
Scenario 2: Incapability with EU standards.....	82
Conclusion.....	83
Recommendations	85
Annex 1 - Terminology.....	89
References	91



List of abbreviations

AKCESK	The National Authority for Electronic Certification and Cyber Security
AKEP	Authority of Electronic and Postal Communications
AKSHI	National Agency of Information Society
AKSIK	National Authority of Classified Information Security
AKSK	The National Authority on Cyber Security
CERT-EU	Computer Emergency Response Team for EU institutions, bodies and agencies
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIO	Operator of the Critical Information Infrastructure
CNI	Critical National Infrastructure
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act (DORA)
eID	Electronic identification
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
ENISA	European Union Agency for Cybersecurity
ENISA	European Union Agency for Cybersecurity
EUROJUST	The European Union's Judicial Cooperation Unit
Europol	European Union Agency for Law Enforcement Cooperation
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
III	Important Information Infrastructure
IIIO	Operator of the Important Information Infrastructure
IIIs	Important Information Infrastructures
ISO	International Organization for Standardisation
ISP	Internet Service Provider
ITU	International Telecommunication Union
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
NCSS	National Cyber Security Strategy
NGOs	Non-governmental organizations
NIS	Networks and Information Systems
OSCE	Organisation for Security and Cooperation in Europe
SCADA	Supervisory Control and Data Acquisition
SOCs	Security Operation Centres



Executive Summary

In 2024, Albania will mark a decade since acquiring the title of an “*official candidate country*” from the European Union (EU).¹ In this decade, Albania has accomplished several milestones in its accession journey toward the EU, culminating with the opening of the EU accession negotiations in July 2022.² EU accession negotiations is a stringent process, in which a country is examined whether they have completed the conditions set by the Treaty on European Union to be admitted to the EU.³

In July 2022, the screening process began for Albania.⁴ The screening process is a crucial step in assessing a candidate country's readiness to adopt and implement the EU *acquis*. Under the new enlargement methodology, the accession process changed, grouping the negotiating chapters into thematic clusters, namely a whole area, which includes the rule of law; internal market; competitiveness, and inclusive growth; green agenda and sustainable connectivity; resources, agriculture and cohesion, and external relations.⁵

Cluster 1 chapter “*Fundamentals First*” contains the following chapters of the EU *acquis*: Chapter 23 ‘Judiciary and fundamental rights’, Chapter 24 ‘Justice, Freedom and Security’, Chapter 5 ‘Public procurement’, Chapter 18 ‘Statistics’ and Chapter 32 ‘Financial Control’, as well as economic criteria; functioning of democratic institutions, and public administration reform. This Cluster will be opened first and closed last.⁶

Chapter 24 ‘Justice, Freedom and Security’ underlines the EU’s aim to “*maintain and further develop the Union as an area of freedom, security and justice*”.⁷ Although not explicitly mentioned in the European Neighbourhood Policy and Enlargement Negotiations (DG NEAR)⁸, the *cyber* element is increasingly becoming a critical aspect within the scope of ‘Justice, Freedom, and Security’ in the European Union.⁹ As technology advances and cyber threats evolve, **the EU recognizes the significance of addressing cybercrime, cyberwarfare, and cybersecurity to safeguard its citizens, institutions, and critical infrastructure.**¹⁰ Albania, as an official candidate country for EU membership, is required to align its administrative

¹ European Council of the European Union, ‘EU enlargement policy: Albania’. Every link is last accessed on 30 September 2023. <https://www.consilium.europa.eu/en/policies/enlargement/albania>

² *ibid.*

³ European Council of the European Union, ‘Enlargement and Stabilisation and Association Process’, 2019. <https://data.consilium.europa.eu/doc/document/ST-10555-2018-INIT/en/pd>

⁴ European Commission.

⁵ European Commission, ‘New enlargement methodology’, 2020.

⁶ *ibid.*

⁷ European Neighbourhood Policy and Enlargement Negotiations (DG NEAR), ‘Chapters of the *acquis*’. https://neighbourhood-enlargement.ec.europa.eu/enlargement-policy/conditions-membership/chapters-acquis_en

⁸ *ibid.*

⁹ European Council of the European Union, ‘Cybersecurity: how the EU tackles cyber threats’. <https://www.consilium.europa.eu/en/policies/cybersecurity/%3e>

¹⁰ European Commission, ‘Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience’, 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2243



and institutional infrastructure and adopt EU legislation, including cybersecurity measures, to meet the criteria set forth by the Treaty on European Union.

In reviewing its past EU Cybersecurity Strategy in 2017, the EU found that (i) *cooperation in matters related to cybersecurity*, (ii) *capacity to prevent, detect, and resolve large scale cyber-attacks*, (iii) *cooperation and information sharing between different stakeholders*, (iv) *protection of critical infrastructure from cyber-attacks* and (v) *research, knowledge, and evidence to support policy action*, were the most urgent gaps and needs.¹¹ To address these issues, the new EU Cybersecurity Strategy presented at the end of 2020 with concrete recommendations for EU Member States in three areas:

resilience, technological sovereignty, and leadership;

operational capacity to prevent, deter and respond; and

cooperation to advance a global and open cyberspace.

The new EU Cybersecurity Strategy¹² initiated a snowball effect of new regulation, directives and proposals, with EU taking a comprehensive and overarching approach to tackle cyber-threats and increasing the cyber resilience of its essential entities across the Union. Possibly, the most important change to note is the repeal of the *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 Directive)* and the adoption of *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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)*.

What has changed?

Amendments	Old EU Standard	New EU Standard
Scope	In NIS1 Directive, it was required for cybersecurity measures to be taken in seven sectors, such as: energy, transport, banking, financial markets, infrastructure, drinking water, healthcare and digital infrastructure.	In NIS2 Directive, the scope is expanded to include: energy (hydrogen & district heating and cooling), wastewater management, digital infrastructure (such as DNS service providers, data centres service providers, cloud computing or content delivery networks), ICT service management, public administration, space, food (production, processing, and distribution), manufactures of medical devices (computer and electronics, machinery and equipment, motor

¹¹ Commission Staff Working Document, 'Proposal for a Regulation of The European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")', 2017.

¹² European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 2020.



		<p>vehicles and other transport equipment), chemicals, digital providers (online marketplaces, search engines and social networking service platforms) and research organisations.</p> <p>States are allowed to go beyond this list.</p>
Risk assessment and mitigation	<p>NIS1 required Operators of Essential Services (OES) and Digital Service Providers (DSP) to carry out a risk assessment of their information and communication systems (ICS) at least once every two years.</p>	<p>Under NIS2, there will be stricter cybersecurity obligations and more rigorous supervisory and enforcement measures (in Albania, from AKCESK). The management bodies of the entities above will have new governance and accountability obligations and can be held liable if the entity fails to comply with security obligations.</p> <p>Plus, NIS2 requires that the members of the management bodies will need to follow cybersecurity training to improve their understanding of cybersecurity risk-management practices.</p>
Incident reporting	<p>Required OES and DSPs to report all significant cybersecurity incidents to their national cybersecurity authority (NCA) within 24 hours of becoming aware of them. A significant incident was one that was likely to have a significant impact on the availability, integrity, or confidentiality of the organization's ICS.</p>	<p>Requires all organizations covered by the directive to (i) notify the relevant supervisory authority or the CSIRT within 24 hours, (ii) submit an incident notification within 72 hours, and (iii) submit a final report no later than after one month with a detailed description of the incident, type of threat or root cause, mitigation measures, and cross-border impact.</p>
Notification to customers	<p>NIS1 did not require OES or DSPs to notify their customers of any cybersecurity incidents.</p>	<p>A new obligation is introduced for entities to notify the recipients of their services of any significant cybersecurity incidents that are likely to have a negative impact on their services.</p>
Enforcement	<p>In NIS1, the EU Member States had discretion to lay down the rules on penalties applicable to breaches of security measures or other obligations set in the Directive.</p>	<p>NIS2 foresees greater enforcement powers of national supervisory authorities. It requires the MS to expand the supervisory authorities' competences to conduct on-site inspections and targeted security audits, request for information, to access data or to request evidence of implementation of cybersecurity policies, and in case of not compliance, even suspend the certification authorisation (court order), and prohibiting the CEO or legal representative of the entity to perform certain duties.</p>



		<p>Furthermore, a key novel thing introduced by NIS2 is the <i>effective, proportionate and dissuasive</i> measures in case of breach of security measures.</p> <p>Entities that fall in the scope of the Directive can expect a fine:</p> <p>Up to EUR 10 million or 2% of annual global turnover for essential entities; and</p> <p>Up to EUR 7 million or 1.4% of annual global turnover for important entities.</p>
--	--	---

Besides the NIS2 Directive, the EU has added upon the existing cyber-acquis by introducing an array of new initiatives, such as: the Cybersecurity Act¹³, Directive on the resilience of Critical Entities Resilience (CER)¹⁴, proposal on Cyber Resilience Act (CRA)¹⁵, Digital Operational Resilience Act (DORA)¹⁶, eIDAS 2.0 proposal¹⁷, and a plan to launch a network of Security Operations Centres across the Union¹⁸. A brief presentation of the benchmarks introduced by these EU initiatives are as follow:

Under the Cybersecurity Act, ENISA has become a permanent agency with a stronger role, as well as a new uniform cybersecurity certification framework for products and services is introduced.

The Critical Entities Resilience Directive (CER) complements NIS2 and lays down new rules on the security and resilience for a list of services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment, including: energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space sector, and production, processing and distribution of food sector (non-exhaustive list).

The proposal for a regulation on cybersecurity requirements for products with digital elements - Cyber Resilience Act (CRA), entails that the manufactures of hardware

¹³ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

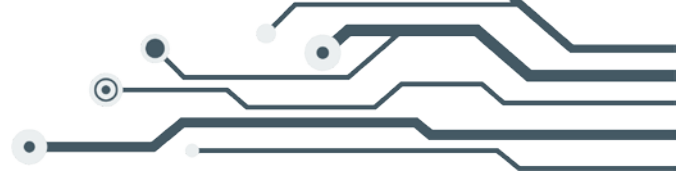
¹⁴ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

¹⁵ Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

¹⁶ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

¹⁷ Proposal for a *Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, COM/2021/281 final.

¹⁸ Press Release, *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*, 2020.



and software services will need to think of cybersecurity-as-design (since the design and development phase and throughout the whole life cycle) and enhance the transparency of security properties of products with digital elements, among other things.

The Digital Operational Resilience Act (DORA) raises the obligation for financial institutions to follow rules for the protection, detection, containment, recovery, and repair capabilities against ICT-related incidents. Generally, it is acknowledging the financial institutions would allocate a capital to manage any operational risk. DORA is applied to critical third parties which provide ICT (Information Communication Technologies)-related services to financial entities. Critical third-country ICT service providers to financial entities in the EU will be required to establish a subsidiary within the EU so that oversight can be properly implemented.

The eIDAS2 will introduce a uniform regulation on the creation and use of digital identities, and the EU citizens will be granted a European Digital Identity, which will function as an ID, driving licence, health record, digital travel document - all in one place.

The Commission has also proposal to launch a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), conceptualised as a 'cybersecurity shield' for the EU, in order to detect signs of a cyberattack early enough and to enable proactive action, before damage occurs.

To comprehend the intricacies and challenges of Albania's cyber landscape, it is imperative to consider the broader context outlined in the EU's approach to cybersecurity. We take this as a comparison model of Albania's cyber landscape.

This study focuses in providing an overview of Albania's cybersecurity landscape that will provide valuable insights into the country's existing strengths and areas that require attention and development. It serves as the cornerstone for Albania's commitment to improving its cybersecurity posture and ensuring a safe digital future within the European Union.

In this context, understanding the broader landscape of Albania's cybersecurity becomes paramount. As Albania advances on its path toward EU membership and endeavours to align its cybersecurity infrastructure with EU standards, it is essential to gauge the current state of its digital defences, the resilience of its critical infrastructure, and its capacity to combat cyber threats effectively.



Main findings and recommendations

The research findings reveal that there is a considerable level of awareness about cybersecurity challenges in the researched setting. However, it is evident that while awareness is present in Albania, there is a glaring misalignment between the EU current cybersecurity policy and Albania's cybersecurity policy.


Finding 1: The Draft Law on Cybersecurity currently in the Parliament lacks some of the key elements introduced in the NIS2 Directive, such as: (i) the uniform methodology to identify the essential entities inside the scope of the Directive, instead of a methodology that will be approved by the National Authority on Certification and Cybersecurity (AKCESK) - as well as the obligation of the essential entities to check in their own if they fall inside the scope of the Directive and report themselves to AKCESK; (ii) a clear set of the obligations of the essential entities instead of broad law provisions that will be followed by a sub-legal act by AKCESK; (iii) the lack of the information obligation of essential entities to report to their users on a critical incident; (iv) not granting more enforcement powers to AKCESK, in particular to prohibiting the CEO or legal representative of the entity to perform certain duties as set in the NIS2; and (v) the non-compliance with the model of fines introduced by the NIS2 Directive. The introduction of the huge fines under the NIS2 Directive is likely to be a significant motivating factor for ensuring compliance with the new standards for the essential entities.

After consultation with AKCESK, it was confirmed that the parliament and the authority seek a near full compliance with the NIS 2 Directive, as amendments to the Draft Law include:

- ✚ A uniform methodology that shall be applied after the approval of the cybersecurity, which will be approved by decision of the Council of Ministers, in line with the NIS2 Directive and EU guidelines;
- ✚ The identification of operators of critical and important information infrastructures will be carried out on the basis of the abovementioned methodology;
- ✚ In the revision of the draft law, there will be a clear set of obligations of CIIOs and IIIOs set in the body of the law;
- ✚ The obligation to notify the public is also foreseen as a new obligation in the revision of the draft law on cybersecurity;
- ✚ AKCESK shall have to prohibit it the CEO or legal representative of the entity to perform certain duties as set in the NIS 2 Directive; and
- ✚ Fines are escalated to 1M-10M ALL.¹⁹

Finding 2: The roles of AKSHI, AKCESK and AKEP need to be clarified if they have double oversight in the critical infrastructures they supervise, particularly on compliance with security measures. According to the current law, AKCESK plays the role of National CSIRT and serves as a Main Point of Contact, also is in charge for implementation of National Strategy. According to experts at AKCESK, in the revision of the draft law on cybersecurity, In the new cyber law: AKEP and AKSHI take the

¹⁹ This information was provided to us by AKCESK, in consultation with the experts working in the new revision of the draft law on cybersecurity.

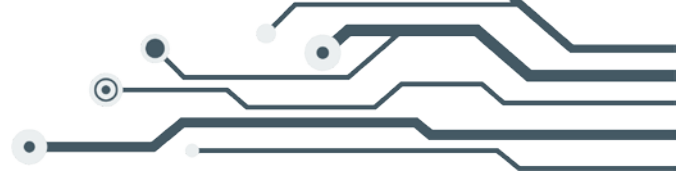


role of Sectorial CSIRTs, and AKCESK has redefine the roles and responsibilities of national stakeholders in the new cyberlaw.

Finding 3: In the last year, AKCESK had the highest increase in human resources among public entities. According to the current Law on Cybersecurity, AKCESK has competence to define cybersecurity measures that *Critical Information Infrastructure Operator* (CIIOs) and *Important Information Infrastructure Operator* (IIIOs) need to adhere to, as well as the methodology of documenting these measures. In analysing the work of AKCESK in the last 2022, specifically relating to the audit of the compliance of security measures of CIIOs and IIIOs is a matter for concern and improvement. In the last year, AKCESK has audited only 8% of CIIOs and 5% of IIIOs in the implementation of security measures. In terms of evaluating the security of CII and IIIO Operators on their emergent security measures, AKCESK has audited 42 CII Operators (out of 73 CII - 57%) and 29 IIIO Operators (out of 89 IIIO Operators - 32%). According to the annual report, the sector on the management of cyber crisis has conducted pentests on CIIOs and IIIOs and conducted research on the field of cybersecurity. These kinds of reports would be immensely valuable to the public, if they could be made to the public in AKCESK website.

Finding 4: Besides the annual reports that provide a more general overview of the fulfilment of the work objectives, AKCESK, ASKHI (National Agency for Information Society) and AKEP (Electronic and Postal Communications Authority) lack publications and research on their respective fields or supporting the entities under their umbrella with country-specific threat assessment reports, guidelines, and updates, like ENISA or Information System Authority of the Republic of Estonia do. In reality, **there is a lack of understanding on the threat landscape in Albania.** Besides the data we have from international indexes, like the Global Cybersecurity Index, or the National Cyber Security Index (which mostly check the countries' policies or laws), there is no research facility, either inside these institutions or independent, that research the state of cybersecurity in Albania, the relationship between stakeholders, the implementation of the laws in practice, what are the threats pertinent to Albania, what can Albania do specifically to address such threats, and to even go deeper in sector-specific research. All the scholar debate on cybersecurity is made on a *vacuum* caused by the lack of such reports and research. In a consultation with AKCESK, AKCESK notes that they prepare every three months periodic report but there not publicly available due to the Confidentiality of information that these reports content have. However, following the practice of ENISA, and other cybersecurity agencies in the EU, these reports could be shared on annual or periodically basis, covering what are the sectors most vulnerable to cyberattacks, what technology are the cybercriminals using to exploit vulnerabilities in the system.

Finding 6: The Critical and Important information infrastructure list that is proposed by AKCESK, audited by AKCESK, and approved by a Decision of Council of Ministers at least once in two years, does include the CIIOs and IIIOs in the relevant sectors defined in the Law on Cybersecurity. However, with the new expanded scope introduced in the NIS2 Directive, additional CIIOs and IIIOs need to be included in the list.



Finding 7: Given the global nature of cyber threats, international cooperation is paramount. In light of recent cyberattacks in the Western Balkans, Albania can navigate the possibility to collaborate with neighbouring countries and international partners to share information, intelligence, and best practices. Cooperation can help identify common vulnerabilities, understand emerging threats, and develop robust defence strategies. Currently, Albania has a Memorandum of Understanding with the Regulatory Authority of Electronic and Postal Services Kosovo, and Agency for Electronic Communication of North Macedonia. Further cooperation could be aimed with other countries in WB, but also in condominium together.

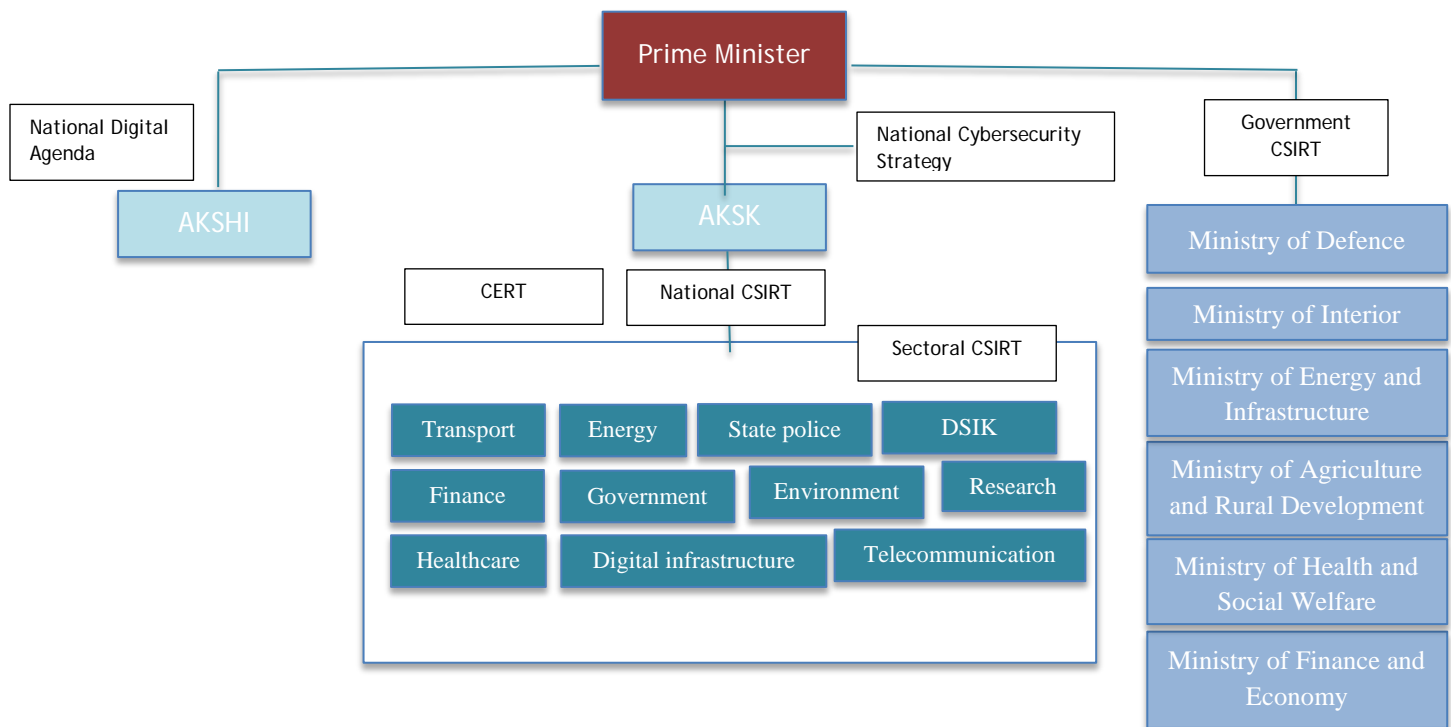
Finding 8: Albania's aspiration to join the European Union necessitates aligning with EU cybersecurity standards. Failure to do so may hinder future negotiations. Key considerations include: *(i) Not aligning with EU standards could result in Albania's cybersecurity infrastructure lagging behind EU counterparts; and (ii) Compliance with EU standards are a critical component of the Accession Negotiations process, and non-alignment may hinder progress.*

Finding 9: Although the Ministry of Defence has taken a proactive role in cyber defence, in creating the cyber unit within the armed forces, the EU cyber defence policy has expanded and focusing on a close civil-military cooperation in the cyber domain.

Finding 10: The cyber governance model in Albania is difficulty understood, even after the collective apprehension of the laws and sub-laws related to cybersecurity in Albania. The current National Cyber Security Strategy lacks a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination, the single points of contact, and the CSIRTs, as well as coordination and cooperation between competent authorities, as required in the NIS2 Directive.

Although the cybersecurity governance framework is not defined by cybersecurity strategies as the competences, roles, and responsibilities of institutions in the field of cybersecurity are defined by law, introducing a governance model in the new National Cybersecurity Strategy would be beneficial and compliant to the requirements of NIS 2 Directive.

Figure 1: Albanian cybersecurity governance according to the draft law.



Source: Own compilation based on the Draft Law on Cybersecurity.

According to AKCESK, in regard to the National Cyber Security Strategy, the institutions which are responsible for its implementation, implement the actions defined in the respective Action Plan 2020-2025, which has recently been revised for the period 2023-2025. The revised Action Plan 2023-2025 is currently going through the required process, in order to be approved by a Decision of the Council of Ministers.

Based on these findings, the **recommendations** set forward are:

The Albanian institutions need to make more effort to enhance the resilience of the critical infrastructures of Albania, through introducing new obligations and measures in alignment with the NIS2 Directive, as well as increasing the scope of what is considered as critical and important infrastructure. Being comprehensive would translate in these entities strengthening the security of their operations, and as a result, securing the infrastructure in case of a cyberattack.

The government needs to allocate more resources and budget specifically for cybersecurity initiatives, research, and infrastructure development. Adequate funding is essential to implement cybersecurity measures effectively. AKCESK needs to invest more resources in auditing the compliance of CIIIs and IIIOs with the security measures in place and conduct regular cybersecurity assessments and audits to identify vulnerabilities and areas for improvements.

The government is recommended to establish uniform cybersecurity requirements for organisations in the financial sector and critical third-party service providers, in accordance with the new EU requirements (DORA), as well as to invest in securing



the digital identities of Albanian citizens by supporting initiatives like the European Digital Identity Wallet (EUDI Wallet). In working towards the EU standard, meaning that the digital identities will be secure, reliable, and compliant with EU regulations, this will be a checked box when Albania heads to Cluster 3.

There is a necessity to increase investment in cybersecurity research, cyber assessments, workforce development, and emerging technologies to bolster Albania's cyber resilience. Albania currently does not have any cyber risk assessment reports, publicly available, that could provide insights on the level of vulnerability against cyber threats, or areas that are most critical to focus.

There needs to be a specific regulation for critical infrastructure in Albania, akin to the EU's regulations, with the aim to provide clarity and guidance to Critical Information Infrastructure Operators (CIIOs) and Important Information Infrastructure Operators (IIIOs) on how to secure infrastructures.

AKCESK needs to strengthen its oversight role in monitoring and enforcing cybersecurity measures among CIIOs and IIIOs. This includes conducting regular audits and assessments to ensure compliance with cybersecurity requirements.

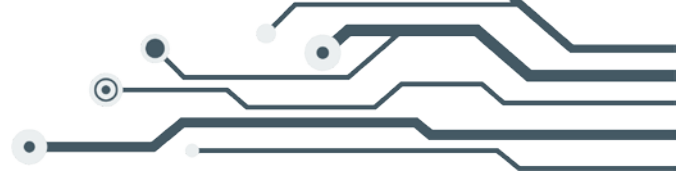
AKCESK needs to explore venues to position itself as a hub for stakeholders to get guidance and support on cybersecurity risk management, incident response, and best practices. AKCESK could explore the possibility of developing clear guidelines and standards tailored to the specific needs of critical infrastructure sectors in Albania

Although Albania is not yet an EU member state country, CIIOs and IIIOs are recommended to proactively begin the compliance with the new standards, as a test run when these requirements will come into power.

Ministry of Defence is recommended to encourage cooperation between the MoD and AKCESK and national CERT, conducting cyber operations and exercises, and blueprints to coordinate during a cyber crisis. The Ministry of Defence is recommended to conduct trainings and explore the Cyber diplomacy toolbox.

The EU is focusing on enhancing the resilience of the critical infrastructures at EU level and Member State level, through new obligations and measures that need to be taken by essential entities and government. For this reason, the PM is recommended to recognise cybersecurity as a national priority and integrate it into broader national security and digital transformation strategies.

Embracing the Digital Operational Resilience Act (DORA) proposal to establish uniform cybersecurity requirements for organisations in the financial sector and critical third-party service providers, the government is recommended to invest in securing the digital identities of Albanian citizens by supporting initiatives like the European Digital Identity Wallet (EUDI Wallet). In working towards the EU standard, meaning that the digital identities will be secure, reliable, and compliant with EU regulations, this will be a checked box when Albania heads to Cluster 3.



Overall, it is recommended that the parliament needs to consider the evolving EU *acquis* in the field of cybersecurity when consulting the adoption of the draft laws currently in parliament. This proactive approach will help prevent discrepancies between Albania and the EU, fostering cooperation and investment opportunities while effectively countering cyber threats. Moreover, any new or revised cybersecurity legislation needs to include clear and detailed obligations for CIIOs and IIIOs, to be compliant with the NIS2 Directive. These obligations need to encompass risk assessment, incident reporting, and compliance with specific cybersecurity measures.



Introduction

This policy paper analyses Albania's path towards European Union (EU) membership, with an emphasis on its cybersecurity policies and their alignment with the evolving EU *acquis*. As Albania approaches a decade as an official EU candidate nation, the research delves into the complex process of EU accession discussions, which demand harmonisation with the EU legal and regulatory requirements. Clustered within the "Fundamentals First" thematic area, cybersecurity has become an integral part of Chapter 24 "Justice, Freedom and Security". The paper emphasises the importance of cybersecurity in the context of the EU's increased focus on protecting digital systems and information.

By drawing parallels between the EU's new cybersecurity strategy and Albania's cyber governance model, the study proposes a strategic realignment of Albania's cybersecurity approach. This recommendation arises from the potential risks of stagnation in cybersecurity progress or incompatibility with current EU standards if Albania adheres to the prior framework.

The European Union has prioritised the task of *Shaping Europe's Digital Future*, by promoting cyber resilience, safeguarding communication and data and keeping online society and economy secure. Over a span of five years, the EU adopted the Second EU Cyber Security Strategy 2020-2025 (EUCSS), adopted the NIS2 Directive on measures for a high common level of cybersecurity across the Union (2022) and is discussing the proposals for the Directive on the resilience of critical entities, a proposal to establish the digital wallet and e-Identity (eIDAS 2.0), and a proposal to set uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies), such as cloud platforms or data analytics services (Digital Operational Resilience Act (DORA)); and other initiatives such as the EU Cyber Diplomacy and expanding the prerogatives of ENISA (The European Union Agency for Cybersecurity). The analysis on EU cyber landscape is based on four pillars:

Pillar 1: Cybersecurity Strategy and Governance

Pillar 2: Investment and Research

Pillar 3: Policy Guidance and Coordination

Pillar 4: Collaboration and Diplomacy

The central focus of this paper is linked to the EU's pivot to another standard of cybersecurity. Considering this, Albania finds itself in the position of pursuing alignment with a moving train (EU trajectory to the Digital Europe). This situation prompts an inquiry into Albania's strategies and measures concerning the resilience of its critical infrastructures and, by extension, its overall approach to cybersecurity.



The aim of this paper is threefold:

To introduce the Albanian audience to the EU standard on cybersecurity;

To provide an overview of the current situation of the cybersecurity in Albania, focusing on the legal framework, cyber policy, cyber resilience of the critical and important information infrastructures; and

To ascertain whether Albania should jump in the EU's moving train towards a resilient, digital society.

The recommendations provided in this policy paper reflect the flow of the European policy and are based on the obligations and recommendations that the EU has introduced to the Member States. In this regard, the author of this policy paper highlights these recommendations to the authorities responsible for security, the operators of critical and important infrastructure and potential critical entities, with the aim to reevaluate the cyber landscape in Albania in order to reflect the EU's vision in it.

Methodology

The overall approach of this paper is based on a qualitative comparative analysis of existing and former EU *acquis*, *vis-à-vis* with the cyber-related legal framework of Albania.

Data sources and validation

The study relies on a blend of quantitative and qualitative research methods to achieve its objectives. The main methods applied here are:

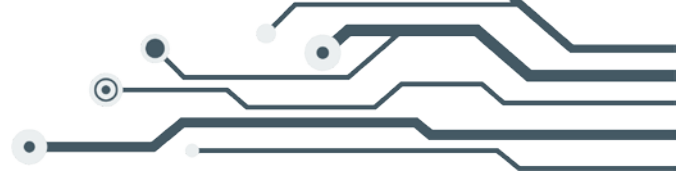
Desk reviews of legislation, regulations, reports, and relevant legal documents; *

Review of cases and samples of government documentation;

Analysis of administrative data from public registries and national and international statistics.

By combining these methods, the paper aims to create a comprehensive assessment of the alignment between the EU's cyber-related *acquis* and the legal framework in Albania. This methodology enables the identification of areas of convergence, discrepancies, and potential gaps, thus contributing to a nuanced understanding of the current state of cyber governance in Albania.

* The primary sources of this paper are laws, regulations, reports and other relevant documents that are publicly available, through institutional webpages of the authorities and stakeholders analysed in this policy paper. Every reference is opened and analysed for the last time on 30 September 2023.



This paper is structured as follows: The first section provides a general look in Albania's cyber situation, focusing on its ranking in world standards such as the Networked Readiness Index, National Cyber Security Index, and Global Cybersecurity Index. Following this, the study goes in depth in the EU cyber landscape, focusing the analysis under four pillars that construe the new developments in EU level in the field of cybersecurity, namely (i) Cybersecurity Strategy and Governance, (ii) Investment and Research, (iii) Policy Guidance and coordination, and (iv) Cooperation and Diplomacy. Through this analysis, we establish the benchmarks introduced in the EU *acquis*, which will help us to understand where Albania stands in terms of alignment with these benchmarks. The next section focuses on Albania's cyber landscape, specifically in the legal framework that governs cybersecurity in Albania, the cybersecurity strategy, cyber resilience, and infrastructure protection and institutional landscape. In this section, we compare almost all the elements that make the cyber governance in Albania, under the lenses of the new adopted directives and proposals. Finally, the study focuses on the scenarios that could arise from taking a decision to align or not with the EU *acquis* at this moment of reforming our cyber governance. Two possible scenarios: One, we decide to continue to the plans and align our laws, institutions, and procedures with the old and repealed EU standard, and possibly lag in the security of the critical and important information infrastructures. Two, as a consequence to adhering to a standard which is not enforced or encouraged in EU level, Albania risks the possibility of not being aligned with the EU.



A brief cyber assessment of Albania

Albania recognises seven sectors as critical infrastructures. These are energy, transportation systems sector, banking sector, financial, healthcare, water systems, and digital infrastructures.²⁰ In this paper, we will analyse what Albania considers critical infrastructures, their importance, the regulations in place, the security measures they need to comply and a brief comparison between Albania and other nations.

Critical infrastructure is defined as “an asset or system which is essential for the maintenance of vital societal functions”..²¹

A good exercise to understand the critical aspect of the critical infrastructures is to question “*What would happen if this facility would not be disrupted for a couple of hours, but for a couple of days?*”..²² For example, if a power plan goes down for a couple of hours, that would not necessarily be a problem. However, if the condition would go for days, weeks or months, the impact on the lack of electricity would impede the functioning of the government, hospitals, transport, and largely and exponentially, affect every aspect of living in today’s interconnected society.

Critical Infrastructure (CI) and Critical Information Infrastructure (CII) are two distinctive notions. To explain, critical infrastructure is defined as “*Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences*”..²³, whereas critical information infrastructure means “*[the] material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic wellbeing of citizens and the efficient function of a country’s government*”..²⁴

²⁰ Law No 45/2019, On Civil Protection.

²¹ European Commission, Critical Infrastructure. <https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure>

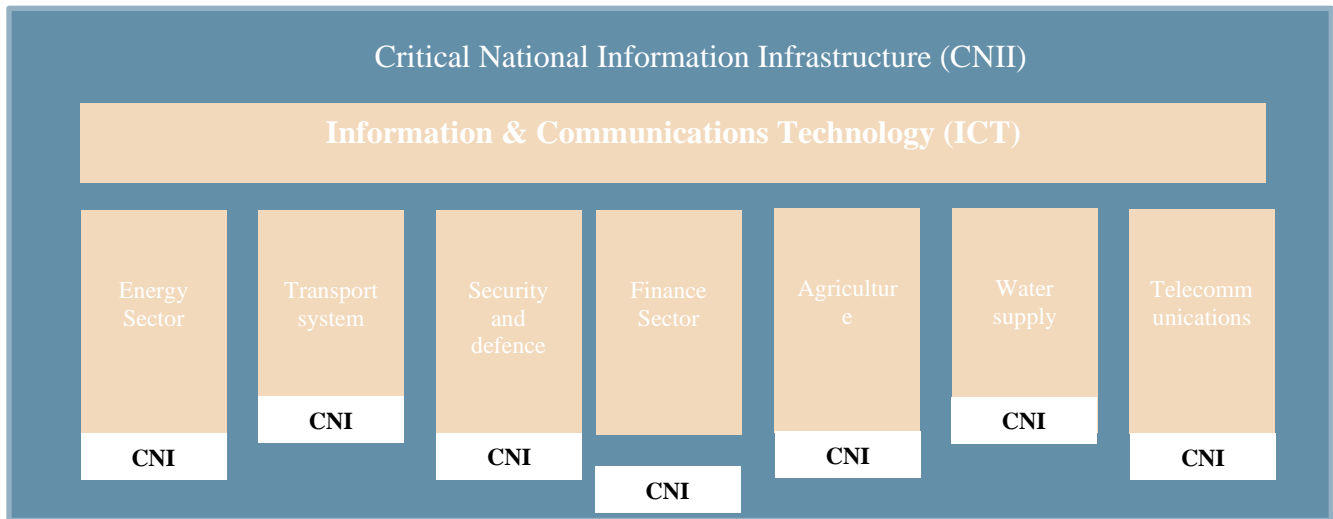
²² UtilSec, [Infovideo Critical Infrastructure Sectors for ICS/OT Cyber Security](https://www.youtube.com/watch?v=YmedABQthec), YouTube. <https://www.youtube.com/watch?v=YmedABQthec>

²³ Global Forum on Cyber Expertise (GFCE), cited in A Boyd, P Victor, E Prasad, 'Introduction to Critical Information and Protection' (ITU), 2020. [https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/Pacific Drill 2020/CII-Protection-ITU-Pacific-Drill-Dec-2020-Final.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/Pacific%20Drill%202020/CII-Protection-ITU-Pacific-Drill-Dec-2020-Final.pdf)

²⁴ International CIIP Handbook 2008/2009, cited in *ibid*.



Figure 1: Critical National Information Infrastructure



Source: ITU, adapted to Albania.

The concept of Critical National Information Infrastructure (CNII) and Critical National Infrastructure (CNI) are not widely encountered in Albania, as the Albanian legislation refers only to Critical Information Infrastructures and Important Information Infrastructure. The distinctive feature according to OECD, is that Critical National Infrastructure “*should focus on the protection of essential services against digital security risk rather than the protection of critical information infrastructures themselves*”.²⁵ To put it in practical terms: In Albania, Korporata Elektroenergjitiqe Shqiptare (KESH), part of the energy sector, which is the public producer and, at the same time, the largest electricity producer in Albania²⁶, should not only focus on protecting the ‘System ABB Symphony SCADA’ and ‘the network of data transmission KESH’ - which are considered as critical information systems in accordance to DCM No 761/2022. But KESH should focus in protecting their whole operations against digital security risk, that could be a malware or bug that interrupts the service of the plants and disrupts the services - which may not be entirely connected to information system. The current legal framework on cybersecurity in Albania does not regulate specifically the protection of critical infrastructures, or critical and important entities. The current law on Cybersecurity²⁷, and the draft Law on Cybersecurity²⁸, leave the critical and important entities outside the scope of regulation, focusing only on the Critical Information Infrastructure and Important Information Infrastructure.

It is important to regulate both the concept of critical infrastructures and critical information infrastructure in Albania. Critical Infrastructure threat landscape is wider than that of the Critical Information Infrastructure, meaning that it could

²⁵ OECD 2015 Security Risk Recommendation, cited in ITU 2020.

²⁶ KESH, Facts about KESH. <https://www.kesh.al/en/about-us/about-kesh/facts-about-kesh/>

²⁷ Law No 2/2017 On Cybersecurity.

²⁸ Draft law On Cybersecurity, Konsultimi Publik. <https://konsultimipublik.gov.al/Konsultime/Detaje/626>



include like terrorist attacks, natural disasters, and more. In the Albanian legal framework, the definition of the “critical infrastructure” is included in the Law No 45/2019 “On Civil Protection”, where critical infrastructures are defined as “*physical structures, networks and other assets, which are essential for the economic and social functioning of the society or community*”.²⁹ According to Article 43 of this law, the critical infrastructure consists of energy (including electricity, oil, gas; telecommunications (networks, systems); water supply; agriculture, food production and distribution; public health (hospitals, health centres and ambulances); transport systems (fuel supply, railway network, airports, ports, internal transport); financial services (banking, clearing) and security and defence services.³⁰

On EU level, Germany has had a National Strategy for Critical Infrastructure Protection since 2019.³¹ In the region, Kosovo has a law on critical infrastructure which regulates the critical infrastructures and their management, including risk management, security plans, roles and responsibilities and sanctions for noncompliance.³²

In the case of Albania, the lack of a law on critical infrastructures and the regulation in singularity of critical (or important) information infrastructures has created the following conundrum: On the List of Critical Information Infrastructures and Important Information Infrastructure³³, Operatori i Shpërndarjes së Energjisë Elektrike (OSHEE), is considered both an Operator of Critical Information Infrastructure and an Operator of Important Information Infrastructure. According to the Law No 2/2017, an Operator of Critical Information Infrastructure is “a legal entity, public or private, that administrates a critical information infrastructure”³⁴, whereas an Operator of Important Information Infrastructure is “a public legal entity, that administrates an important information infrastructure”.³⁵ The difference between an important and critical information infrastructure is on the result element in case of an attack to the information system. If, an attack against the network and system would have an impact in the health, security, or economic wellbeing of citizens, that information network is considered critical. However, if there are networks that are not part of this category, but an attack to these networks would bring a significant disruption or hindrance to the work of the public administration, then this is considered an Important Information Infrastructure. On EU level, the difference between the operators of critical and important infrastructures is not only conceptual, but also relate to the level of adherence to

²⁹ Law No 45/2019, On Civil Protection, Article 3, para 15.

³⁰ *ibid*, Article 43.

³¹ Federal Ministry of the Interior and Community, National Strategy for Critical Infrastructure Protection (CIP Strategy), 2019.

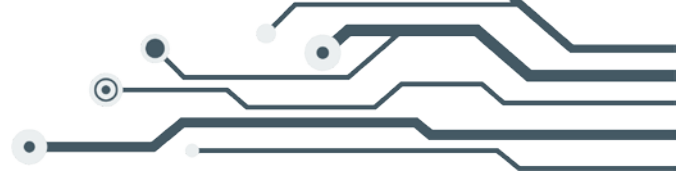
https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html;jsessionid=41788FA1A20963642FE911DD9DE20B06.1_cid360

³² Law No 06/L-014 on Critical Infrastructure.

³³ DCM No 761/2022, On some Additions and changes in the Decision No 553, dated 15.7.2020, of the Council of Ministers, “On the approval of the list of the Critical Infrastructures of Information and Important Infrastructures of Information”.

³⁴ Law No 2/2017 On Cybersecurity, Article 3, para 8.

³⁵ Law No 2/2017 On Cybersecurity, Article 3, para 9.



security measures. In the current legislation in Albania, there is no distinctive elements proscribed in any of the articles. The differences between the two operators are not reflected either in the Draft law on Cybersecurity. The issues connected to this *lacuna* in law be analysed further in the study.

As mentioned above, we have two divergences between critical infrastructures and critical information sectors, one designated by the DCM No 761/2022, and one by the Law No 25/2019.

DCM No 761/2022 on the List of the Critical and Important Infrastructures	Law No 25/2019 on Civil Protection
<i>Sectors where we can find Critical and Important Information Infrastructures</i>	<i>Critical Infrastructures</i>
Energy	Energy
-	Telecommunication
Water supply	Water supply
-	Agriculture
Transportation system	Transportation system
-	Financial services
-	Security and defence
Banking	-
Healthcare	-
Digital infrastructure	-

Table 1: Critical Infrastructures provided in the DCM No 761/2022 and Law No 25/2019.

Source: Own compilation.

According to the Law No 2/2017 On Cybersecurity, the Authority responsible on Electronic Certification and Cybersecurity (AKCESK), sends the list on the Critical and Important Information Infrastructures at least once in two years to the Council of Ministers for approval. The current list was updated in 2022.³⁶ AKCESK has a Methodology to identify and classify Critical and Important Information Infrastructures.³⁷ A six-pager methodology notes the criteria and factors to identify and classify information infrastructures, as below:

³⁶ DCM No 761/2022.

³⁷ AKCESK, Decision No 9, dated 14.2.2022. <https://cesk.gov.al/wp-content/uploads/2023/09/Metodologjia.pdf>



Criteria	Factors
Economic impact	Financial effect - caused by the disruption of the infrastructure
Political/governmental impact	Time effect - defined in hours, days, months and years, since the disruption of an infrastructure
Industrial/environmental impact	Geographical effect - number of individuals affected by the malfunctioning of the infrastructure
Health Impact	

Table 2: Criteria and factor to identify and classify information infrastructures.

Source: AKCESK, Methodology. <https://cesk.gov.al/wp-content/uploads/2023/09/Metodologjia.pdf>

Interestingly, in the methodology, AKCESK has defined 12 sectors of critical and important of information, namely (1) Energy, (2) ICT, (3) Water, (4) Food, (5) Healthcare, (6) Financial services, (7) Public Order and Safety, (8) Transport, (9) Industry, (10) Civil Administration, (11) Space, (12) Civil Protection, (12) Environment, and (14) Defence. Meaning that if we add an extra column to *Table 1*, we go to the conclusion that an Order of an Agency, has a wider scope than the law and a DCM.

DCM No 761/2022 on the List of the Critical and Important Infrastructures	Law No 25/2019 on Civil Protection	Order No 9, dated 14.2.2022
<i>Sectors where we can find Critical and Important Information Infrastructures</i>	<i>Critical Infrastructures</i>	<i>The methodology on the identification and classification of the critical and important infrastructures of information</i>
Energy	Energy	Energy
-	Telecommunication	Telecommunication (ICT)
Water supply	Water supply	Water supply
-	Agriculture	Agriculture
Transportation system	Transportation system	Transportation System,
Financial services	Financial services	Financial Services
-	Security and defence	Security and defence
Banking	-	Banking
Healthcare	-	Healthcare



Digital infrastructure	-	-
-	-	Public Order and Safety
-	-	Chemical Industry and nuclear
-	-	Civil Administration
-	-	Civil Protection
-	-	Environment

Table 3: Critical Infrastructures provided in the DCM No 761/2022, Law No 25/2019 and AKCESK methodology to identify critical information infrastructures.

Source: Own compilation.

The inclusion and exclusion of sectors is not a matter of just listing entities as critical, important or neither. If an operator falls within the sector and fulfils the criteria defined in the law, or in the order of AKCESK in this instance, the Operator of the Critical Information Infrastructure (IIIO) and the Operator of the Important Information Infrastructure (IIIO) must adhere to the security measures set by AKCESK³⁸, failure of which could provide the basis for an administrative offence³⁹, and result on an administrative sanction⁴⁰ to the operator for failure to complying with the law.

The prerogative of AKCESK to define in its own the critical sectors, when the law has left it unregulated, could constitute a hindrance to the principle of legal certainty. Meaning, the law on this field needs to be certain, foreseeable, and easy to understand. For this reason, Albania needs to adopt a law on critical infrastructure abiding to the EU and international standards, clearly stating which are the critical sectors, and which are the criteria to define the critical and important entities within these sectors.

Based on the Law No 2/2017 On Cybersecurity, we understand the following cybersecurity governance model:

³⁸ Law No 2/2017, Article 8, para 2. CIIOs and IIIOs “are obligated to adhere the security measures [set by AKCESK - Article 5/a] and document their implementation”.

³⁹ *ibid*, Article 21. 1. In terms of this law, the following violations constitute administrative offenses:

- a) non-reporting of cyber incidents (...)
- b) non-fulfilment of the obligations set by [AKCESK] (...)
- c) non-reporting to the Authority of the point of contact or their updates (...);
- ç) non-fulfilment of the obligations defined within the corrective measures (...).

⁴⁰ *ibid*, Article 22. “When [AKCESK] finds a violation of the provisions, which constitute an administrative offence, according to Article 21, of this law, imposes the following penalty:

- a) from 200,000 to 800,000 ALL, in case of administrative violations defined in letters "a" and "ç" of point 1;
- b) from 20,000 to 40,000 ALL, in case of administrative violations defined in the letter "c" of point 1;
- c) from ALL 40,000 to ALL 200,000, in case of defined administrative violations in the letter "b" of point 1.



The key stakeholders mentioned in the law are: AKCESK, CIIOs, IIIOs, the Council of Ministers, the Minister responsible for the field of Information and communication technologies.

CIIOs and IIIOs are identified and classified pursuant to the List of the Critical and Important Information Infrastructures, proposed by AKCESK and approved by the Council of Ministers. According to the DCM No 761/2022, the current sectors where we can find the Critical and Important Information Infrastructures are energy, transportation services, banking, financial services, water supply, and digital infrastructure. Currently, there are 77 CIIOs and 81 IIOs (*note that there are Operators who fall in both categories, as the categorisation is made on whether they have an important or critical infrastructure; some operators have both*).

Each CIIOs must have a designated cyber security specialist, who will have a dual role as part of the Computer Security Incident Response Team (CSIRT).⁴¹ Meanwhile, IIOs must have only one person responsible of cyber security incident.

Both CIIOs and IIIOs must comply with organisational and technical measures, which are defined by AKCESK.

In the case of a cyber incident, AKCESK is the point of contact on national and international level. It coordinates the response against a cyber incident and assists the operators in the countermeasures, among other things.⁴²

In the case of a state of cyber crisis⁴³, the Minister responsible for ICT proposes to the Council of Ministers to declare the state of cyber crises. The duration of the state of cyber crisis can be seven days, which can extend only by approval of the Prime Minister. However, the state of cyber crises cannot extend beyond 30 days.⁴⁴ During this state, the responsible minister for ICT (note here: the current responsible minister in Albania, which can include ICT to some extent, is the Minister on Infrastructure and Energy), proposes solutions to the Prime Minister on resolving the state of the cyber crisis.⁴⁵

The Law no 2/2017 is considered as not adequate to effectively respond to the challenges posed to the security of networks and information systems in Albania.⁴⁶ For this reason, AKCESK has proposed a Draft Law on Cybersecurity, which as of 2022, is currently under discussion in the Parliament. The Draft Law on Cybersecurity foresees clearer legal provisions that regulate AKCESK, National CSIRT,⁴⁷ sectorial CSIRT,⁴⁸ and the CSIRTs near the operators of the Critical Information

⁴¹ Law no 2/2017, Article 7, para 2.

⁴² *ibid*, para 5.

⁴³ The state where the information security in information systems or the security of telecommunication networks is seriously endangered, putting the public interest of the Republic of Albania at risk.

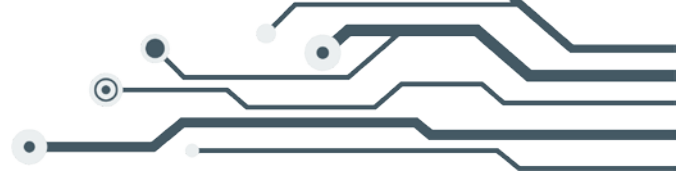
⁴⁴ Law no 2/2017, Article 19

⁴⁵ *ibid*, Article 19, para 2.

⁴⁶ Report on the Draft Law on Cybersecurity, p 2.

⁴⁷ Cyber Security Incident Response Team, at AKCESK. Draft law on Cybersecurity.

⁴⁸ The Cyber Security Incident Response Team for operators of critical and important information infrastructures. Draft law on Cybersecurity.



Infrastructures⁴⁹.⁵⁰ Furthermore, it provides the establishment of a structure, National SOC, who will conduct the monitoring of security on a national level. The study will focus on the analysis on the draft law at a latter moment. What is important to note in this instance is that the draft law follows the NIS 1 Directive⁵¹, whereas this Directive has been repealed in 2022.

The whole conundrum to the cyber landscape in Albania is the lack of legal clarity, and the lack of a realist approach to cybersecurity. At the time of the study, neither AKCESK nor any other public or private entity has produced a threat landscape report identifying threats, trends with respect to threat actors and attack techniques, and relevant mitigation measures personalised to Albania. AKCESK Annual Reports⁵², do provide the data gathered from the monitoring sessions from AKCESK. However, these data are not sufficient to create a complete picture. Without a thorough awareness of the threat landscape, engaging in cybersecurity policymaking becomes a difficult task fraught with uncertainty and potential pitfalls.

Regarding Albania's cyber policy framework, we can form an understanding based on international indexes.

Albania is ranked 80th in the Networked Readiness Index (NRI)⁵³, 54th in the National Cyber Security Index⁵⁴, and 80th Global Cybersecurity Index.⁵⁵ Through a cross cutting-analysis of these indexes, the overall conclusion is that Albania overall cybersecurity readiness and policy framework need improvement.

The Networked Readiness Index which ranks a total of 131 economies based on their performance across 58 variables, has ranked Albania (i) 94th in the level of technology that is *essential* for a country's participation in the global economy (technology pillar), (ii) 48th in the availability and level of technology in a country (people pillar), (iii) 92nd in how safe individuals and firms are in the context of the network economy, regulation and digital inclusion (governance pillar) and (iv) 79th on the impact that readiness has had on the growth and well-being in society and the economy (impact pillar).⁵⁶ Through an arbitrary look of the NRI, Albania is not performing well in the pillar of *technology* and *governance*. Within these categories, recommendation arise related to (i) adoption and investment in emerging technologies in the country, (ii) facilitating online access to financial account and

⁴⁹ The cyber security incident response person/team, for the relevant sector, located near an operator that manages critical and important information infrastructures, or the responsible institution of the line. Draft law on Cybersecurity.

⁵⁰ Report on the Draft Law on Cybersecurity, p 2.

⁵¹ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS 1).

⁵² AKCESK, Annual Reports, 2022, 2021, 2020.

⁵³ Albania's position in the NRI reflects its preparedness and ability to leverage digital technologies effectively. This index assesses a nation's capacity to utilize information and communication technologies to enhance competitiveness and socioeconomic development. Link <https://networkreadinessindex.org/>

⁵⁴ This index evaluates the nation's cybersecurity readiness, policy frameworks, and measures in place to safeguard against cyberthreats.

⁵⁵ Overall cybersecurity preparedness. This index takes into account a broader range of factors, including legal frameworks, technical capabilities, and strategic initiatives aimed at managing and mitigating cyber risks.

⁵⁶ Network Readiness Index, Albania Report, 2022. <https://networkreadinessindex.org/country/albania/>



(iii) lowering the socioeconomic gap in use of digital payments, among many other things.⁵⁷ These gaps are not in the focus of this paper. Despite this, gaining an understanding on Albania's challenges to leverage information and communication technologies is closely connected to the wider context of cybersecurity. Overall, Albania is placed 40th in Europe and behind its region in all four pillars.⁵⁸

Albania's ranking of 54th in the National Cyber Security Index (NCSI) for the year 2022 indicates its relative performance compared to other countries in terms of cybersecurity readiness to counter cyber threats.⁵⁹ While Albania may perform well or at an average level in several NCSI indicators, there are specific areas of concern that could potentially impact its overall cybersecurity posture, namely *cyber threat analysis and information* (0%), *cyber crisis management* (20%) and *military cyber operations* (0%).⁶⁰ A 0-20% score indicates that these areas lack attention by the official entities. Addressing these areas can contribute to improving Albania's cybersecurity infrastructure, enhancing its ability to protect against cyber threats, and ensuring the effective management of cyber incidents to safeguard critical systems and data.

In the Global Cybersecurity Index 2020, Albania is ranked 80th out of 132 countries at the global level and 40th out of 46 countries at the European level, based on an evaluation of cybersecurity measures taken by the country.⁶¹ Notably, Albania demonstrated relative strength in the realm of *Legal Measures*, while there exists considerable potential for growth in the domain of *Cooperative Measures*.⁶² The harmonisation of national legislation with Council of Europe treaties and European Union directives has a significant impact on the development of the legal framework for cybersecurity.⁶³ Ratification of the Convention on Cybercrime and its Additional Protocol has influenced how the standards it establishes for cybercrime and electronic evidence are represented in national criminal legislation. However, a score of 64.32 indicates that Albania's cybersecurity measures should be improved.

As mentioned above, there is lack of data and research, and as a result, a clear understanding of the vulnerabilities and the level of threshold against cyberattacks of the critical and important infrastructures in Albania. In Ireland's National Cyber Risk Assessment 2022, it is noted that there is and will continue to be an increase in state-sponsored actor trends which try to exploit zero-day and other critical vulnerabilities; as well as a growing interest of state actors in targeting critical infrastructure and operational technology; and increased focus on supply chain compromises.⁶⁴ Other threats mentioned are disruptive operations against

⁵⁷ This is also recommended by the European Commission in the Screening Report.

⁵⁸ Network Readiness Index, Albania Report, 2022.

⁵⁹ National Cyber Security Index, Albania, 2022.

⁶⁰ *ibid.*

⁶¹ ITU, Global Cybersecurity Index. Albania. 2020. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>

⁶² *ibid.*

⁶³ Council of Europe Portal. Octopus Cybercrime Community. Albania. <https://www.coe.int/en/web/octopus/-/albania>

⁶⁴ Government of Ireland, National Cyber Security Centre, *National Cyber Risk Assessment 2022*, p 5.



organisations⁶⁵, espionage by nation-state actors⁶⁶, state-backed groups engaging in cybercrime⁶⁷, hybrid warfare⁶⁸ and other threats. This kind of exercise - if it were to be conducted by AKCESK, would provide a great amount of clarification and understanding for the public and researchers on the state of vulnerability of the country against cyber threats.

In EU level, the European Union Agency for Cybersecurity (ENISA) publication "Foresight 2030 Threats", has put forward that EU (and the world for that matter) can expect threats from state-sponsored actors inserting a backdoor in an online code repository as a mean to acquire information to blackmail leaders, espionage, or otherwise initiate disruptions across the EU, to manipulation of systems necessary for emergency response, like ambulances, police, firefighters, etc..⁶⁹ Although an assessment of this nature is not available tailored to Albania, the global nature of cybercrime does allow us to make an assumption that Albania might be victim of similar threat scenarios.

In regard to law and policy, Albania has a Law on cybersecurity⁷⁰ and several fragmented regulations that refer to cybersecurity issues.⁷¹ Essentially, the legal framework that governs cybersecurity in Albania excludes the electronic communications⁷², protection of personal data⁷³, crime in the cyberspace⁷⁴, electronic signature⁷⁵, electronic commerce⁷⁶, electronic document⁷⁷, electronic

⁶⁵ *ibid.* The report mentions the deployment of destructive malware such as WhisperGate and HermeticWiper against organisations in Ukraine to destroy computer systems, as well as the attack on the Viasat satellite network which caused communication outages and disruptions across several public authorities, businesses and users in Ukraine. The report mentioned the cyber-attacks as well that destroyed data and disrupted essential government services, including paying utilities, booking medical appointments and enrolling schoolchildren (attack on e-Albania), and leaked Albanian government data.

⁶⁶ Advanced Persistent Threats (APTs) that targeted government institutions and political organisations in the European Union and Member States, as well as key European industries.

⁶⁷ As a revenue generation activity.

⁶⁸ According to the report, adversaries have increasingly invested resources to target ICS (Industrial Control System), which as a cause to the digital transformation initiatives, the rise of Industrial IoT, the cloud connectivity of ICS devices, as well as the remote access services for ICS networks, have become more vulnerable to such attacks.

networks

⁶⁹ ENISA, *Foresight 2030 Threats*.

⁷⁰ Law no 2/2007, On Cybersecurity.

⁷¹ M Bada, F Hammed, *Report on Cybersecurity Maturity Level in Albania (January 15, 2019)*, Available at SSRN: <https://ssrn.com/abstract=3658345> or <http://dx.doi.org/10.2139/ssrn.3658345>, p 54.

⁷² Law No. 9918 from 19.05.2008, On electronic communications.

⁷³ Law No. 9887 from 10.03.2008, On protection of personal data.

⁷⁴ Law No. 7895 from 27.01.1995, Criminal Code of Albania, Law No. 7905 from 21.03.1995, Criminal Procedure Code of Albania (in compliance with the Council of Europe Cybercrime Convention).

⁷⁵ Law No.9880/2008, On electronic signature.

⁷⁶ Law No.10128/2009, On electronic commerce.

⁷⁷ Law no 10273/2010, On electronic document.



identification and trust services⁷⁸, and e-governance⁷⁹, which are regulated in different laws.⁸⁰

In policy level, the Albanian government is focused in enhancing infrastructure and bolstering the capabilities of governmental bodies, enhancing the quality of public services and digital governance, and overseeing the online services and digital economic market.⁸¹ The main strategic documents on cybersecurity are The National Cybersecurity Strategy and its Action Plan 2020-2025⁸² focusing in cybercrime, radicalism, violent extremism, and protection of children on the internet; the National Strategy for Cyber Defence 2021-2023⁸³ which focuses in the national defence of the country; and the Intersectoral Strategy 'The Digital Agenda of Albania' 2022-2026 which focuses on the digitalisation process of the public services and infrastructure.⁸⁴

Currently, there is no entity within the Albanian government with centralised and policymaking competencies in cybersecurity, ICT, electronic communications, or media.⁸⁵ Technical agencies, rather than policymakers, are currently the primary stakeholders in cybersecurity governance. They are made up of institutions from the central government (the prime minister's office and ministries) and their subordinate agencies, as well as independent institutions.⁸⁶ The cybersecurity governance landscape is made of the following stakeholders: The National Authority for Electronic Certification and Cybersecurity (AKCESK), the National Agency for Information Society (AKSHI), the Electronic and Postal Communications Authority (AKEP), cybercrime units in the Albanian State Police and the Prosecution offices, Ministry of Defence, and responsible Minister on ICT - currently Ministry of Infrastructure and Energy. The cyber governance model and the relationship between these stakeholders will be analysed further in this paper.

The key theme of this paper is the cyber governance challenges in Albania, particularly in enhancing the resilience and protection of the critical and important informational infrastructure, in accordance with the EU standards. To reiterate, (i) Important Information Infrastructure (hereinafter referred to as IIIs) are *"the entirety of networks and systems information owned by a public authority, which is not part of the critical infrastructure of information, but that could jeopardize*

⁷⁸ Law no 107/2015, On Electronic Identification and Trust Services.

⁷⁹ Law no 43/2023, On electronic governance.

⁸⁰ Law no 43/2023, On electronic governance.

⁸¹ DCAF, Cybersecurity and Human Rights in the Western Balkans: Mapping governance and actors, M Reçi, S Kelmendi, Chapter 1: Albania, Bridging the gap between cyber policy fragmentation and human rights, p 9. https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityHumanRightsWesternBalkans_EN_March2023.pdf

⁸² DCM No 1084, On the approval of The National Cybersecurity Strategy and its Action Plan 2020-2025, dated 24.12.2020. https://cesk.gov.al/wp-content/uploads/2020/07/strategjia_kombetare_sigurise_kibernetike-1.pdf

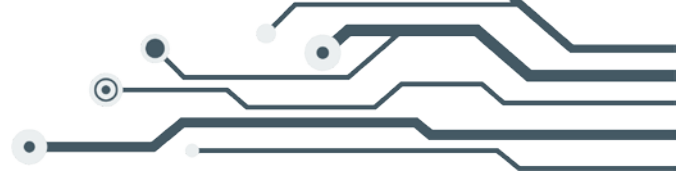
⁸³ Ministry of Defence, the National Strategy for Cyber Defence 2021-2023.

<https://www.mod.gov.al/images/PDF/2020/Strategjia-Mbrojtjen-Kibernetike-2021-2023.pdf>

⁸⁴ DCM No 370, On the approval of the Intersectoral Strategy 'The Digital Agenda of Albania' and the action plan 2022-2026, dated 1.6.2022. <https://akshi.gov.al/wp-content/uploads/2022/06/vendim-2022-06-01-370-Agjenda-Digjitale-e-Shqiperise-22-26-dhe-plani-i-veprimit.pdf>

⁸⁵ DCAF study, p 10.

⁸⁶ *ibid.*



or limit the work of the public administration in the event of information security breaches", whereas (ii) Critical Information Infrastructure (hereinafter referred to as CIIs) are "the entirety of networks and systems information, the violation or destruction of which would have a serious impact on health, security and/or economic well-being of citizens and/or the effective functioning of economy in the Republic of Albania".⁸⁷ The critical sectors covered by the law no 2/2007 On Cybersecurity in Albania are: energy, transport, drinking water, digital infrastructure, financial markets, banking and health sector. In 2022, there are 77 Critical Information Infrastructure Operators (CIIOs) and 81 Important Information Infrastructure Operators (IIIOs). Technological advancement and widespread interconnectedness that characterise today's critical and important information infrastructures provide the path for new vulnerabilities. CIs are highly vulnerable to cyber-attacks, and particularly threatened by the 'cascading failure' phenomena, which involves the risk that failure in a single component of a given infrastructure could lead to the failure of additional components.⁸⁸ Digitalisation and the growing reliance of these infrastructure on web services and connected networks, calls for governments to have an *all-hazards approach* when working to enhance the resilience of critical infrastructures; meaning, taking into account man-made, technological threats and natural disasters in the critical infrastructure protection process.⁸⁹

In conclusion, Albania's cybersecurity landscape presents a mix of strengths and challenges that require a concerted effort to align with EU standards and enhance its digital resilience. As Albania continues its path toward EU membership, addressing these cyber governance issues will be pivotal to ensure a secure digital future within the European Union.

In the following section, we will delve into the new standards and directives introduced by the EU, followed by how Albania aligns with these evolving requirements and the progress it has made toward fulfilling the criteria set by the EU on its path to membership.

⁸⁷ Law No 2/2017, On Cybersecurity, Article 3.

⁸⁸ P Tessari, K Muti, Study, 'Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations', 2021.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU\(2021\)653637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf)

⁸⁹ *ibid*, p 55.



The EU cyber landscape

The EU has taken a proactive approach to strengthening cybersecurity landscape across the EU Member States and further. It has been a key priority for the EU to safeguard data across multiple sectors that have been through a period of digital transformation including economics and politics, finance, healthcare, energy, and education.⁹⁰

Over the past five years, the European Union has seen a substantial transformation in its cyber infrastructure. This includes the adoption of the Network and Information Security Directive NIS2 Directive⁹¹, the Critical Entities Resilience Directive (CER)⁹², and Digital Operational Resilience Act (DORA)⁹³, and pushed its agenda further with the proposals eIDAS⁹⁴, and the Cyber Resilience Act (CRA)⁹⁵.

2nd Cybersecurity Strategy (EUCSS)	The Critical Entities Resilience Directive (CER)	The NIS2 Directive	Digital Operational Resilience Act (DORA)	Cyber Resilience Act (CRA)	eIDAS 2.0
The European Cybersecurity Certification Framework.	Each MS shall adopt a strategy for enhancing the resilience of critical entities.	Cybersecurity risk management.	Financial institutions must follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.	Transparency on the security of hardware and software products.	Cross-border digital services (authentication and device identification)
A network of security operation centres	Harmonised rules allowing for a consistent identification of critical entities across the EU.	Reporting obligations.	Uniform requirements concerning the security of network and information systems supporting the business	Security-by-design.	Digital Identity Wallet

⁹⁰ Concilium. Cybersecurity: how the EU tackles cyber threats.

<https://www.consilium.europa.eu/en/policies/cybersecurity/#:~:text=The%20EU%20adopted%20in%202022,by%20the%20COVID%2D19%20pandemic>

⁹¹ Tangible Solutions. Cybersecurity Is Like an Onion, It Has Layers. <https://www.tangible.com/blog/general-hit/cybersecurity-is-like-an-onion-it-has-layers/>

⁹² Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)

⁹³ Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

⁹⁴ Proposal for a Regulation of the European parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

⁹⁵ Proposal for a Regulation of the European parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.



			processes of financial.		
A joint cyber unit.	Critical entities shall take appropriate and proportionate technical and organisational measures to ensure their resilience and shall ensure that these measures are described in a resilience plan or equivalent document or documents.	Improve the resilience and incident response	Almost all financial entities will be subject to the new rules.	Consistent cybersecurity framework that simplifies compliance for both hardware and software producers.	A universal, cross-border e-ID.
Security of 5G networks.		Increase of scope of sectors considered as critical & important (a size-cap rule).	Critical third-country ICT service providers to financial entities in the EU will be required to establish a subsidiary within the EU so that oversight can be properly implemented.		Use products with digital elements securely.
Strong encryption.					
Cyber diplomacy toolbox.					
EU external cyber capacity building agenda.					

Table 4: An overview of key EU cyber legal documents.

Documents highlighted in green indicate their adoption, whereas those in red are presently in the proposal phase.

In October 2020, the EU leaders called for stepping up the EU's ability to (i) *protect itself against cyber threats*, and (ii) *provide for a secure communication environment, especially through quantum encryption ensure access to data for judicial and law enforcement purposes*.⁹⁶ The EU recognises the digital transformation of society has brought new challenges, which require innovative response. In December 2020, the European Commission, and the European External Action Service (EEAS) presented a new EU cybersecurity strategy (EUCSS). The aim of this strategy is to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new strategy contains concrete proposals for deploying regulatory, investment and policy instruments. One proposal was for the EU to amend the legislation for a high common level of cybersecurity across the Union (NIS1), to further improve the resilience and incident response capacities of

⁹⁶ Concilium. Cybersecurity: how the EU tackles cyber threats.

<https://www.consilium.europa.eu/en/policies/cybersecurity/#:~:text=The%20EU%20adopted%20in%202022,by%20the%20COVID%2D19%20pandemic>



both the public and private sector and the EU without disparities in-between them (NIS2 Directive).⁹⁷

EUCSS aims to ensure “a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe”. It covers the security of essential services such as hospitals, energy grids, railways, and the connected objects in our homes, offices, and factories. The strategy aims to build collective capabilities to respond to major cyberattacks. It outlines plans to work with partners around the world to ensure international security and stability in cyberspace.⁹⁸

The EU Cybersecurity Strategy has two focal points: (i) *The European Cybersecurity Certification Framework inclusive of EU-wide certification schemes in a package of comprehensive set of rules, technical requirements, standards, and procedures*⁹⁹; and (ii) *The strengthening of the European Network Information Security Agency (ENISA), the official European Union Agency for Cybersecurity*.¹⁰⁰

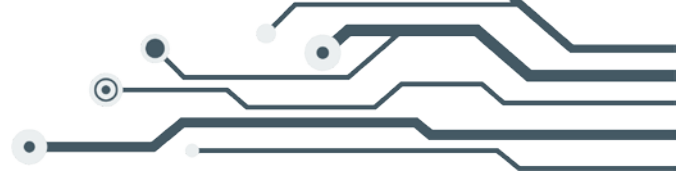
To comprehensively assess the European Union's approach to cybersecurity and to ease our understanding of EU's cyber landscape, we have structured their approach to cybersecurity in four main pillars: (1) Cybersecurity Strategy and Governance, (2) Investment and Research, (3) Policy Guidance and Coordination, and (4) Cooperation and Diplomacy. These pillars serve as the foundation for evaluating the EU's strategies, investments, policies, and collaborative efforts in the ever-evolving landscape of cybersecurity. By delving into each of these pillars, we aim to provide a holistic perspective on how the EU is addressing the challenges and opportunities presented by the digital age; through this, we aim to pinpoint specific aspects in which Albania can align itself with EU standards and best practices.

⁹⁷ European Commission, The EU's Cybersecurity Strategy for the Digital Decade, 2020. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

⁹⁸ *ibid.*

⁹⁹ A uniform Certification Framework EU-wide, which aims to bypass the implementation of different standards in different EU MS for same services.

¹⁰⁰ European Commission. *Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*



Pillar 1: Cybersecurity Strategy and Governance

The expanded threat landscape and the new challenges posed to security in the digital realm, were the main factors which required adapted and innovative response, and henceforth, the adoption of a new EU Cybersecurity Strategy.¹⁰¹ The EU's aim is to lead the efforts for a secure digitalisation and be a leader in driving norms for world-class and standards of cybersecurity of essential services and critical infrastructures, as well as driving the development and application of new technologies. Most importantly, the EU is setting this paradigm in EU level: **governments, businesses and citizens will share a responsibility in ensuring a cyber-secure digital transformation.** This means that the approach to cybersecurity will change from national authorities having the main burden to ensure the cybersecurity of service and digital providers; but such burden will be shared. This approach is logical in front of the uncertainty that technological advancement will bring in the future.

Currently, the EU has built a robust legal *acquis* in relation to the resilience of critical infrastructures, the cornerstone of which rests upon the NIS1 Directive and the Cybersecurity act.¹⁰² The equation is simple: The EU requires member states to define and adopt a national cyber security strategy and designate a competent authority who will constantly monitor the operators who are designated as critical or important to the country. In the NIS1 Directive, the authorities of the member states had leniency to define what falls under the categories of critical and important to the operation of its daily citizens. This brought discrepancies between countries, where an entity or operator that might be considered critical in one member state might not hold the same status in another member state. This could create challenges, especially when such operators were part of supply chains or networks that crossed multiple member states.¹⁰³ For example, consider a scenario where a company providing a vital service was classified as "critical" in one member state but not in another. If this company was part of a supply chain or network that operated across both member states, it could lead to inconsistencies in how cybersecurity and risk management measures were applied to that company. This lack of harmonization could potentially undermine the overall cybersecurity resilience of critical services and infrastructure within the European Union.

With the introduction of NIS 2 Directive, many of the elements of the NIS1 Directive have changed. The table below summarizes the main amendments and new requirements under the NIS 2 Directive:

¹⁰¹ *ibid.*

¹⁰² European Council. EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation.

¹⁰³ European Commission. Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN>



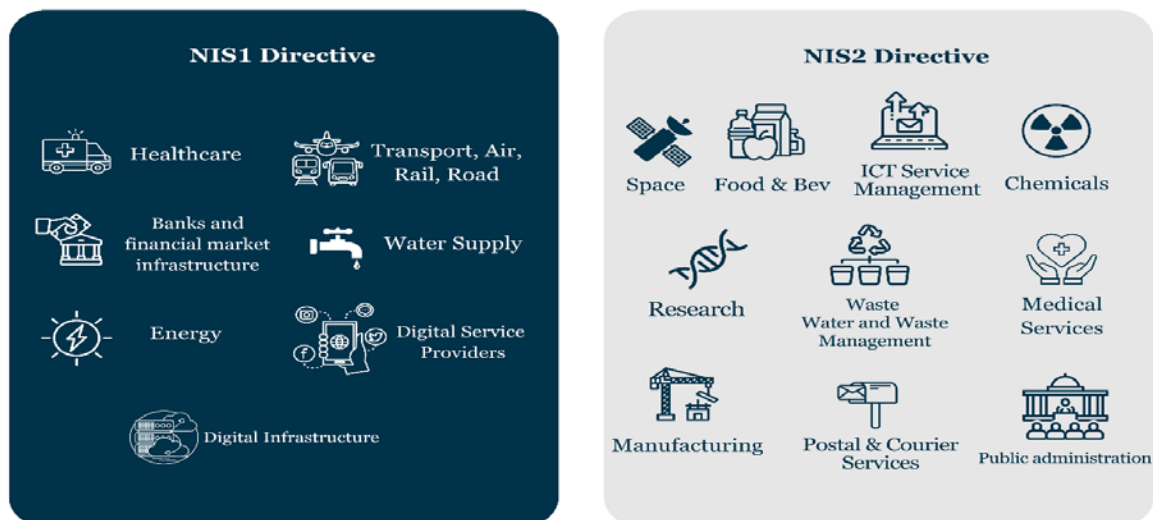
Amendment	NIS1	NIS2
Scope	Applied to operators of essential services (OES) and digital service providers (DSPs).	<p>The NIS 2 Directive expands the scope of application to cover:</p> <ul style="list-style-type: none"> * All medium and large organizations in the following sectors: energy, transport, financial services, healthcare, water, and digital infrastructure. * Smaller organizations in these sectors that are considered to be of high importance due to their critical role in society. * All organizations that provide essential digital services, such as online marketplaces, cloud computing services, and search engines.
Risk assessment and mitigation	Required OES and DSPs to carry out a risk assessment of their information and communication systems (ICS) at least once every two years.	Requires all organizations covered by the directive to carry out a risk assessment of their ICS at least once every two years. The risk assessment must identify and assess the likelihood and impact of potential cybersecurity incidents. Organizations must also take appropriate measures to mitigate the risks identified in their risk assessment. These measures must be proportionate to the risks and must be reviewed and updated on a regular basis.
Incident reporting	Required OES and DSPs to report all significant cybersecurity incidents to their national cybersecurity authority (NCA) within 24 hours of becoming aware of them. A significant incident was one that was likely to have a significant impact on the availability, integrity, or confidentiality of the organization's ICS.	Requires all organizations covered by the directive to report all significant cybersecurity incidents to their NCA within 24 hours of becoming aware of them. A significant incident is one that is likely to have a significant impact on the availability, integrity, or confidentiality of the organization's ICS, or on the provision of essential services.
Notification to customers	NIS1 did not require OES or DSPs to notify their customers of any cybersecurity incidents.	Organisations must notify their customers of any significant cybersecurity incidents that are likely to have a negative impact on their services.
Enforcement	Allowed NCAs to impose fines of up to €10 million or 2% of the organization's global turnover, whichever was greater, for non-compliance.	The NIS2 Directive introduces tougher enforcement measures for non-compliance. Organizations that fail to comply with the directive's requirements may be subject to fines of up to €20 million or 4% of their global turnover, whichever is greater.

Table 5: From NIS1 to NIS2 - what has changed?

Source: Own compilation.

The NIS2 Directive will have a significant impact on the organisations that fall within its purview, how they operate, and the management's accountability for the implementation of cyber security measures.

Figure 2: Added industries under the scope of NIS2



Source: Own compilation.

Entities that operate in the industries above, that employ over 250 people and have an annual turnover of more than EUR 50 million or an annual balance sheet above EUR 43 million are defined as essential services. Irrespective of this criterion, the national authority can designate an entity as critical, if a cybersecurity incident on this entity would cause devastating consequences on health, safety, or the environment.¹⁰⁴

The entities who are designated as critical sectors have until October 2024 to implement cyber security risk management measures to protect the organisation, including abiding by the following obligations:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, including backup management, disaster recovery, and crisis management;
- Supply chain security;
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cyber security risk-management measures;

¹⁰⁴ NIS 2 Directive.



- Basic cyber hygiene practices and cyber security training;
- Policies and procedures regarding the use of cryptography and encryption;
- Human resources security, access control policy, and asset management;
- The use of Multi-Factor Authentication (MFA) and secured emergency communications.¹⁰⁵

If the national authority find that the critical and important entity has not taken the above-mentioned measures noted as the *“appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems”*¹⁰⁶, or failed their reporting obligations to *“notify, without undue delay, its CSIRT or competent authority of any incident that has a significant impact on the provision of their service”*¹⁰⁷, can be subject of an administrative fine of a maximum of at least EUR 10.000.000 for essential entities (7.000.000 for important entities) or of a maximum of at least 2% for essential entities (1.4% for important entities) of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher.¹⁰⁸ Also, although important and critical entities are subject to the same security requirements, when it comes to supervision and enforcement, essential entities are subject of regular, targeted and ad-hoc audits, while important entities are only audited after security incidents.¹⁰⁹

Besides the NIS2 Directive, the EU has added upon the existing cyber-*acquis* by introducing an array of new initiatives, such as a Directive on the resilience of Critical Entities Resilience (CER)¹¹⁰, Cyber Resilience Act (CRA)¹¹¹, Digital Operational Resilience Act (DORA)¹¹² and a plan to launch a network of Security Operations Centres across the Union.¹¹³

Different from NIS2 Directive that focuses on improving the overall cybersecurity posture of the EU by setting cybersecurity standards, requiring incident reporting, and promoting cooperation and information sharing among member states, the Critical Entities Resilience Directive (CER), on the other hand, places specific obligations on member states to ensure that essential services and vital societal functions or economic activities are maintained without disruption in the internal

¹⁰⁵ NIS 2 Directive, Article 21

¹⁰⁶ NIS 2 Directive, Article 21.

¹⁰⁷ NIS 2 Directive, Article 23.

¹⁰⁸ NIS 2 Directive, Article 34.

¹⁰⁹ NIS2 Directive, Article 32 and 33.

¹¹⁰ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

¹¹¹ Proposal for a Regulation of the European parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020/.

¹¹² Proposal for a Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)

¹¹³ European Commission, *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*, 2020.



market. CER Directive focuses specifically on critical entities, which is identified by a Member State following the requirements below:

- the entity provides one or more essential services;
- the entity operates, and its critical infrastructure is located, on the territory of that Member State; and
- an incident would have significant disruptive effects¹¹⁴, on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors that depend on that or those essential services..¹¹⁵

Based on the provisions set in the CER Directive, member states are introduced with these obligations:

Firstly, Member States need to adopt a strategy dedicated strictly to enhancing the resilience of critical entities, which will co-exist with other documents, such as the National Cybersecurity strategy. The resilience strategy should contain measures to aim for a high level of resilience of the critical entities of the sectors covered in the CER Directive¹¹⁶, and be comprehensive to contain a governance framework, a description of measures, a description of the process in which critical entities are identified, and a list of the main authorities and relevant stakeholders..¹¹⁷

Second, after having established a non-exhaustive list of essential services and the strategy, the competent authority needs to do a risk assessment) by 17 January 2026, and after, whenever necessary subsequently, and at least every four years..¹¹⁸

Third, Member States shall establish a list of the critical entities and notify them that (1) they have been identified as critical entities, and (2) that they have obligations.

Under the CER Directive, the competent authorities of Member States shall provide support to critical entities, shall ensure that critical entities take appropriate and

¹¹⁴ Taking into account (a) the number of users relying on the essential service provided by the entity concerned; (b) the extent to which other sectors and subsectors as set out in the Annex depend on the essential service in question; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population; (d) the entity's market share in the market for the essential service or essential services concerned; (e) the geographic area that could be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas;

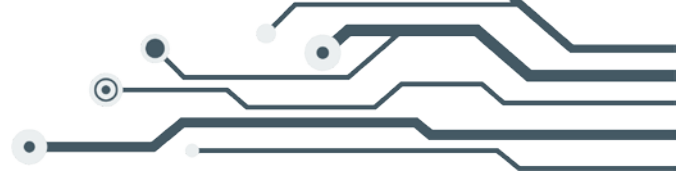
(f) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service. CER Directive, Article 7.

¹¹⁵ CER Directive, Article 6.

¹¹⁶ Critical infrastructures based on the scope of the CER Directive are: Energy, Transport, Banking, Financial market infrastructure, Health, Drinking water, Waste water, Digital infrastructure, Public administration, and Space. CER Directive, Annex.1

¹¹⁷ Proposal CER Directive, Article 4.

¹¹⁸ Proposal CER Directive, Article 5.



proportionate technical, security and organisational measures to ensure their resilience, and run background checks on people who hold sensitive roles in or for the benefit of the critical entity, are authorised to directly or remotely access its premises, information or control systems, or are under consideration for recruitment.¹¹⁹

Dedicating a directive to resilience of the critical infrastructures is a clear indication of EU's aim on strengthening the resilience of its critical infrastructure.¹²⁰ Furthermore, all the studied cyber legal act work in harmony and in complementarity with each-other. For instance, the proposal for the Cyber Resilience Act (CRA) aims to achieve what is called "security-by-design" of the digital products that are made in the EU.¹²¹ The CRA Regulation will be a comprehensive regulation that will contain (i) rules to place products with digital element in Europe; (ii) essential requirements for the design, development and production with digital elements, and obligations for economic operator; (iii) requirements for the vulnerability handling processes, and (iv) rules on market surveillance and enforcement of the abovementioned requirements.¹²²

The EU's process of thought on cyber is to not only work on the front of putting security measures in place, or only focusing on proactively resolving cyber vulnerabilities, but put on a standard on what products with digital elements can be used in the EU. These products with digital elements shall be made available on the market when they meet the requirement set in the proposal CRA Directive, and the manufacturer has complied with the essential requirements of this regulation.

Comprehensive rules governing products with digital elements to guarantee their cybersecurity, encompassing requirements for their design, development, production, and obligations for economic operators. Additionally, it outlines essential criteria for vulnerability handling processes throughout the product lifecycle, along with market surveillance and enforcement measures to ensure compliance with these rules and requirements. Ensuring that every piece of the puzzle that makes the digital society we live in is protected against vulnerabilities and possible cyber-attacks, the EU's approach to achieving this is a wide-ranging one.

eIDAS2 is a proposal regulation aimed to repeal eIDAS1 at the EU level for the same reasons as the NIS1 Directive - essentially, a lack of uniform regulation for trusted identification in the private sector and inconsistencies in using eIDAS services.¹²³ Under the eIDAS2, an EU-level framework on the creation and use of digital identities

¹¹⁹ Proposal CER Directive, Article 14.

¹²⁰ Three areas of EU action – (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace.

¹²¹ Security by design is an approach to product or system development that integrates security measures from the very beginning of the design process. It involves identifying potential security risks and vulnerabilities and implementing measures to mitigate them at each stage of development, rather than trying to add security as an afterthought. This proactive approach aims to create products, systems, or software that are inherently secure, reducing the likelihood of security breaches or vulnerabilities later on.

¹²² Proposal CRA Regulation, p 9.

¹²³ European Commission, Discover eIDAS. <https://digital-strategy.ec.europa.eu/en/policies/discover-eidas>



will be created.¹²⁴ In this framework, the European Digital Identity will be created, that will function as an ID, driving licence, health record, digital travel document - all in one place.

Connected with the reform on the digital identity, the EU plans to launch the European Digital Identity Wallet, which will function as the application used in our phones, as Apple Pay, Samsung pay and Google Pay.¹²⁵ To support the MS in the implementing this new reform, the EU has introduced the EUDI toolbox, which is the core technical architecture and the reference framework needed to implement the European Digital Identity Wallet.¹²⁶ This document will be fully compliant to GDPR and the Cybersecurity Act, as it will be accompanied with strong cryptography and the highest-level assurance against data leaks.¹²⁷ eIDAS2 has foreseen that the security and privacy of electronic identities and trusted services will be strengthened.

The Digital Operational Resilience Act (DORA) proposal aims to set uniform requirements for the security of the networks and information systems of companies and organisations active in the financial sector as well as critical third parties that provide services related to ICTs.¹²⁸ The idea behind this regulatory framework on digital operational resilience is to make sure that IT security of financial entities such as banks, insurance companies and investment firms can withstand, respond to and recover from all types of ICT-related disruptions and threats.¹²⁹

DORA requires financial institutions to follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.¹³⁰ Before DORA, financial entities allocated a capital for covering the traditional risk categories, without necessarily following the cybersecurity measures obligations.¹³¹ Under the requirements that flow from the regulation, the relevant financial authorities¹³² will develop technical standards that all financial services providers must follow.¹³³ The Albanian government and relevant authorities are recommended to be updated on the new standards introduced by the European authorities, and implement them in the national level. Importantly to note now for Albania is that even prior to joining the EU, critical third-country ICT service providers to financial entities in the EU will be required to establish a subsidiary within the EU so that oversight can be properly implemented.

¹²⁴ European Commission, European Digital Identity. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

¹²⁵ European Commission, European Digital Identity Wallet. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3556

¹²⁶ Ibid.

¹²⁷ European Commission, Europe's Digital Decade.

¹²⁸ The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554.

¹²⁹ <https://www.dora-info.eu/>

¹³⁰ <https://www.dora-info.eu/>

¹³¹ PwC, *Introducing the Digital Operational Resilience Act*.

¹³² European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the the European Insurance and Occupational Pensions Authority (EIOPA).

¹³³ The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554.



Pillar 2: Investment and Research

After the pandemic, the EU Commission released its Recovery Plan for Europe - a €806.9 billion investment fund with the aim to *make "Europe greener, more digital and more resilient"*.¹³⁴ In terms of cyber resilience, the EU is using a part of the budget for research and innovation, its digital transition, and for increasing its preparedness, recovery, and resilience.¹³⁵

Horizon Europe and Digital Europe programmes are two EU initiatives aimed at fostering innovation, research, and development in the fields of science, technology, and digitalization.¹³⁶

Through Horizon Europe, the EU's flagship research and innovation program for 2021 to 2027, the EU seeks to provide funding for scientific research, innovation, and technological advancement across various sectors - cybersecurity being one of them. The funding aims to foster the partnerships with the public and the private sector for research and innovation covering digital technologies (photonics, future internet, cybersecurity), HPC, 5G, electronics components and systems, and factories of the future.¹³⁷

Digital Europe program run concurrently with Horizon Europe and is designed specifically to enhance Europe's digital capabilities and competitiveness. It allocates:

€7.5 billion to five areas, namely supercomputing, AI, cybersecurity, advanced digital skills and ensuring a wide use of digital technologies.

Includes the "cybersecurity and trust" pillar - a €1.6 billion fund *"to boost cyber defence and the European Union's cybersecurity industry, finance state-of-the-art cybersecurity equipment and infrastructure and support the development of skills and knowledge"*.¹³⁸

It focusses on promoting digital technologies, infrastructure, and skills across the European Union.

The EU has assessed that to enable the digital transformation Europe needs to first strengthen its digital capacities in High-performance computing (HPC) and data, AI, cybersecurity and trust, and advanced digital skills, and latter to make digital capacities available and deploy them throughout society and economies.

¹³⁴ European Commission. Recovery plan for Europe.

¹³⁵ *ibid.*

¹³⁶ European Commission & European Investment Bank. European Cybersecurity Investment Platform, 2022. <https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf>

¹³⁷ European Commission. Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021–2027. 2018.

¹³⁸ *ibid.*



In essence, through these initiatives, we understand the focus that the EU is giving to increasing cybersecurity and cyber resilience in Europe.

The EU opened its Digital Europe Programme to candidate countries Montenegro, North Macedonia, Albania and Serbia to access calls for funding.¹³⁹ However, AKCESK notes that Regarding the Digital Europe Programme, the program is open to Albania in general, except for calls in the field of cyber security.¹⁴⁰

Albania's participation in calls in the field of cyber security is hindered by the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024 and amending the Commission Implementing Decision C(2021) 7914 on the adoption of the multiannual work programme for 2021-2022.¹⁴¹

In the Annex of this decision, it is stated that participation in the calls funded under this Work Programme will be subject to the provisions of Regulation (EU) 2021/694. Consequently, Albania cannot apply in the cyber security related calls that have been published so far in the framework of this program.

As EU has raised the rhetoric on the Western Balkan possibly joining the Single Digital Market, in areas such as e-commerce or cybersecurity,¹⁴² the inclusion of Albania and other WB in the calls for cybersecurity needs to be a priority for the EU.

¹³⁹ European Commission, Shaping Europe's digital future. Not only the Digital Europe Programme, but also other EU programmes as Horizon Europe, will be available for Montenegro, Macedonia, Serbia, and Albania to apply for funding, these are good opportunities for these countries to invest particularly in resilience and enhancing on the cybersecurity of their critical infrastructures.

¹⁴⁰ Consultation with AKCESK.

¹⁴¹ *ibid.*

¹⁴² Directorate-General for Neighbourhood and Enlargement Negotiations, Keynote speech by President von der Leyen at the GLOBSEC 2023 Bratislava Forum, https://neighbourhood-enlargement.ec.europa.eu/nees/keynote-speech-president-von-der-leyen-globsec-2023-bratislava-forum-2023-0531_en#:~:text=Never%20can%20e%20match%20the,act%20%E2%80%93%20call%20it%20ASAP



Pillar 3: Policy Guidance and Coordination

The standards set by the EU with the adoption of the recent directives and regulations will probably be a challenge for EU member states as much as for the EU candidate countries, like Albania, to implement. For this reason, the EU has worked on the externalities in synchronisation with the legal and policy developments through providing toolbox and supporting guidelines on how to implement the new benchmarks on cybersecurity.

The EU Cyber Diplomacy Toolbox¹⁴³

The Cyber Diplomacy Toolbox is construed as a framework that contributes to conflict prevention by setting out restrictive measures that can be used to prevent and respond to malicious cyber activities.¹⁴⁴ It co-exists with cyber defence, cyber deterrence, and cybersecurity, and aims to create "an open, free, stable and secure cyberspace anchored in international".¹⁴⁵ Through this toolbox, EU highlights that cyber diplomacy is as an important aspect as deterrence of enhancing the cybersecurity of a country. In particular now, as cyber space is considered the fifth domain of warfare.¹⁴⁶, and under the increasing number of cyberattacks, prioritising international cooperation on cyber norms, resilience and responsible behaviour in cyberspace is given utmost importance.

Blueprint for coordinated response to major cyber-attacks.¹⁴⁷

A plan that applies to cybersecurity incidents which cause disruption affecting two or more MS or EU institutions with a wide-ranging significant impact. Principally, in case of an EU-wide crisis with cyber elements, the Council will be the coordinating body - and the crisis response mechanisms will be activities. The Blueprint notes how this mechanism will make use of existing cybersecurity entities at EU level as well as cooperation between the Member States and focuses more on the response part of the cyber crisis.

The central mechanism for cooperation in the Blueprint is the CSIRTs Network, chaired by the Presidency and with secretariat provided by ENISA. In the Blueprint, a lesson to be taught by the cooperation between the actors is that it is done on three levels:

Level 1: Cooperation at the technical level

Level 2: Cooperation at the operational level

¹⁴³ Council Decision (CFSP) 2019/797 Of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

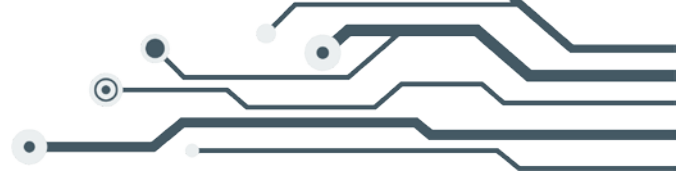
¹⁴⁴ *ibid*, p 1.

¹⁴⁵ EU policy brief, Understanding the EU's approach to cyber diplomacy and cyber defence.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI\(2020\)651937_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf)

¹⁴⁶ NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

¹⁴⁷ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incident and crises. Blueprint for coordinated response to major cyber-attacks.



Level 3: Cooperation at the strategic/political level.¹⁴⁸

Through engaging all the relevant stakeholders in these three levels, the Blueprint and the EU seeks to facilitate comprehensive and effective cooperation in addressing cybersecurity challenges.

EU Cyber Defence policy and the Action Plan on Military Mobility 2.0

The recent attacks on critical infrastructure systems in the EU and in Albania as well, have incited a debate on the possibility of these cyber threats to escalate in a possible act of war. For this reason, the EU has thought to provide a borderless solution to a borderless space as cyberspace. In a case scenario where an adversary can attack energy networks, transport infrastructure and space assets, the EU has thought of cohesive action between citizens, civilian and military operations against cyber threats.¹⁴⁹

The aim is to create a Union-wide 'cybersecurity shield' that will facilitate the detection of cyberattacks and provide an impetus for proactive action.¹⁵⁰ EU bases this policy on four pillars:

- Reinforcement of the coordination mechanisms among national and EU cyber defence players, increasing information exchange between military and cybersecurity and supporting military CSDP missions and operations;
- Further standardisation and certification of non-critical and critical software to secure both military and civilian domains;
- Increasing investment in modern military cyber defence capabilities; and
- building on existing security and defences as well as cyber dialogue with partner countries.¹⁵¹

Taking this approach, the EU signals a new relationship between the civilian and military domain. In order to enhance the protection of EU critical infrastructure, the EU has launched an initiative to promote the deployment of an EU infrastructure of Security Operation Centres (SOCs) made of several multi-country SOC platforms, which will improve the collective detection capabilities of cyber threats.¹⁵² In essence, the policy defines the EU supporting mechanisms in development of specific militaries across the EU, but leaves the responsibility to Member States to use cyber defence capabilities to protect their critical infrastructure, unify the cyber defence capabilities and adapt to the changing geopolitical environment.¹⁵³ Other requirements left at the Member States' playing field based on this policy are:

¹⁴⁸ Blueprint. *ibid.*

¹⁴⁹ European Commission, Cyber Defence: EU boosts action against cyber threats. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642

¹⁵⁰ EU Cyber Direct, European Union.

¹⁵¹ European Commission, Cyber Defence: EU boosts action against cyber threats.

¹⁵² Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, p 6. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber_defence.pdf

¹⁵³ *ibid.*, p 13.



- The necessity for MS to strengthen common situational awareness and coordination within defence community;
- Member States are encouraged to join EU Cyber Defence Coordination Centre (EUCDCC) on EU level;
- Member States are called to participate in MICNET, an operational network for military CERTs.¹⁵⁴

The requirements of MS to explore the collaboration between Computer Security Incident Response Teams (CSIRT) and Military Computer Emergency Response Team Operational Network (MICNET), in joint meetings and exercise, information sharing and incident response efforts.¹⁵⁵

- Enhance cooperation at the strategic, operational, and technical level between cyber defence and other cyber communities;¹⁵⁶
- Increase overall cyber defence maturity at national level;¹⁵⁷ and among many others;
- Enhancing research efforts on key technologies for cyber defence, like AI, encryption, and quantum computing, to ensure that the defence systems remain security after an attack from disruptive technology.¹⁵⁸

This internal build-up of capabilities is supplemented by the development of a specialised 'cyber diplomacy toolbox' that allows the Union and its Member States to address cyber incidents through various joint policies, from cooperation and stabilisation measures to restrictive measures and attribution.¹⁵⁹

As a conclusion, novel elements introduced in the cyber defence in the EU area that Albania can benefit from exploring more are:

- EU Cyber Defence Coordination Centre (EUCDCC) is created to support enhanced situational awareness within the defence community;
- An operational network for milCERTs (Military Computer Emergency Response Teams) is set up on EU level;
- The EU Cyber Commanders Conference;
- A new framework project CyDef-X to support EU cyber defence exercises;
- EU civilian infrastructure of Security Operation Centres (SOCs);
- Information exchange between the cyber defence community and the other cyber communities, and
- A reserve pool of experts from trusted private providers will be created in case of a cyber emergency.¹⁶⁰

¹⁵⁴ *ibid*, p 3.

¹⁵⁵ *ibid*, p 4.

¹⁵⁶ *ibid*, p 7.

¹⁵⁷ *ibid*, p 12.

¹⁵⁸ *ibid*, p 13.

¹⁵⁹ European Commission, Cybersecurity Policies.

¹⁶⁰ Press release, [The EU Policy on Cyber Defence](#), 2022.



EU Toolbox on 5G¹⁶¹

The EU Toolbox on 5G is a set of guidelines and measures developed by the European Union to enhance the security of 5G networks across its member states. The EU Toolbox on 5G sets out a series of security requirements that 5G network providers and operators must adhere to. These requirements aim to safeguard the integrity and resilience of 5G networks against potential cyber threats. The toolbox includes a risk assessment framework that allows EU member states to identify and assess potential security risks associated with 5G networks. It also provides guidance on imposing relevant restrictions on high-risk suppliers, particularly those that may pose security concerns.

The EU Toolbox on 5G provides member states with a coordinated and comprehensive approach to addressing the cybersecurity challenges associated with 5G technology. It enhances the security of critical infrastructure, promotes information sharing, and ensures compliance with EU regulations, ultimately contributing to a more secure and resilient 5G ecosystem across the EU.¹⁶²

¹⁶¹ EU Toolbox For 5G Security, A set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks, 2021. <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>

¹⁶² *ibid.*



Pillar 4: Cooperation and Diplomacy

Cyber diplomacy is a term combining 'diplomacy' and 'cybersecurity', and it is defined as *"the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace that are commonly crystallised in the national cybersecurity strategies"*.¹⁶³ The European Union (EU) actively engages in cyber diplomacy on an international level, promoting the creation of universal norms for responsible behaviour in cyberspace while encouraging cybersecurity cooperation with other countries and areas.¹⁶⁴

The EU Cyber Defence policy framework adopted in 2014, was updated in 2018 to better correspond to the new cybersecurity challenges.¹⁶⁵ Under this, cooperation and conflict resolution in cyberspace are given consideration. The list of priorities has been updated to include research and development, training and drills, technology, civil-military interaction, and international cooperation.¹⁶⁶ Following the state-sponsored cyberattack in 2022, Albania severed the diplomatic relations with Iran, in what is considered the first instance of this occurrence.¹⁶⁷ Albania, like many countries, may engage in cyber diplomacy to collaborate with other nations on cybersecurity issues. For instance, in the case mentioned above, cyber diplomacy would have played a role in how Albania and Iran addressed the aftermath of the cyberattack, including any negotiations or diplomatic discussions related to the incident.

In this context, concern is raised if Albania may find it difficult to keep up with the escalating cybersecurity standards of the EU unless it increases its efforts and concentrates on improving its cyber governance. Based on this premise, the security of Albania's critical infrastructure and its cyber responsiveness will be examined in the context of the future in an attempt to provide solution - oriented recommendations to Albania.

¹⁶³ Australian Institute of International Affairs, Defining Cyber Diplomacy.

¹⁶⁴ EU policy brief, Understanding the EU's approach to cyber diplomacy and cyber defence.

¹⁶⁵ Council, EU Cyber Defence Policy Framework (2018 update).

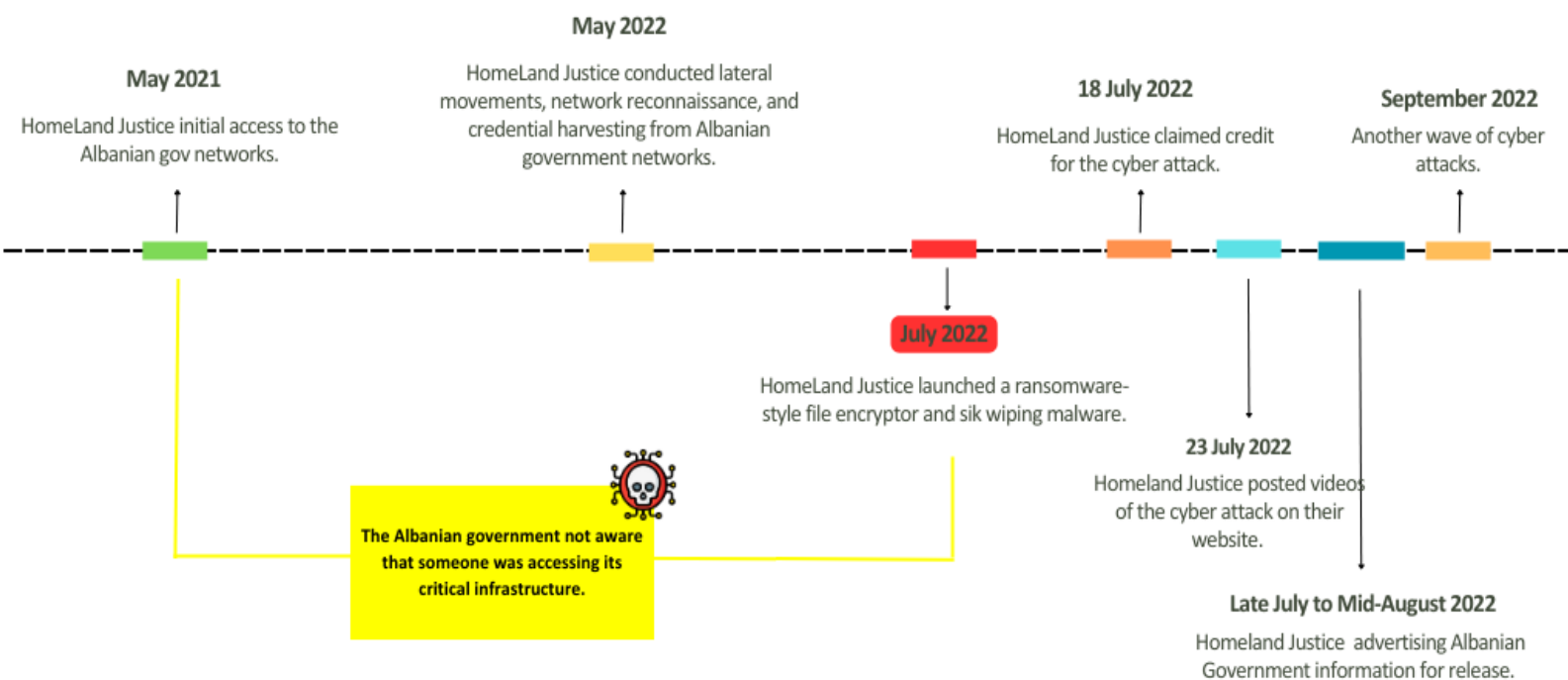
¹⁶⁶ General Secretariat of the Council, EU Cyber Defence Policy Framework (2018 update).

¹⁶⁷ BBC, Albania severs diplomatic ties with Iran over cyber-attack.

Albania's cyber landscape

Albania's approach to cybersecurity can be divided in two periods: pre- and post-2022 data breaches. In 2022, nearly 1 million cyberattacks targeted Albania, where 80% of them had their origin from Iran.¹⁶⁸ The attack on Albania's critical public and private infrastructure paralysed the country, which had recently completed its shift from providing public services from in-person public to virtually. Following the attack, a joint FBI and Microsoft investigation found that the hackers (known as HomeLand Justice group) had infiltrated in the system 9 months before the attack.¹⁶⁹ This moment raised concerns in terms of vulnerabilities of the critical infrastructures and its impact on the real life.

Figure 3: Chronology of the events of the data leaks



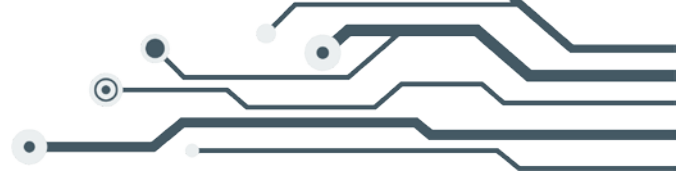
Source: *FBI & CISA Joint Cybersecurity Advisory Report*. 21 September 2022.

The data breaches shifted the government's focus to the critical need for stronger cybersecurity measures and tactics. At the time the cyber-attack happened, Albania was transitioning to an e-government paradigm with the purpose of delivering public services through information computer systems.¹⁷⁰ Following the intrusions, the

¹⁶⁸ KohaJone, Flet “mbreti” i sigurise kibernetike shqiptare. 2023.

¹⁶⁹ The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), Joint Cybersecurity Advisory on Iranian State Actors Conduct Cyber Operations Against the Government of Albania, 2022. <https://www.cisa.gov/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf>

¹⁷⁰ Currently, a new law on electronic governance is adopted. Law No 43/2023 "On Electronic Governance".



country's cybersecurity ecosystem underwent a drastic shift, as seen by an increase in AKCESK budget and personnel numbers, AKCESK activities and projects¹⁷¹, and the submission of a new draught cybersecurity law to parliament, among other things.¹⁷² However, adopting comprehensive cyber governance measures into the country's legal framework and institutional structure presents significant obstacles for Albania, particularly now that the EU has modified its approach to cybersecurity, for the following reasons.

Firstly, as previously noted, Albania is in the midst of reforming its cyber governance in the aftermath of the 2022 cyber-attacks. Albania has an opportunity to strengthen its cyber defence capabilities, improve collaboration with international partners, and develop a comprehensive cybersecurity framework to protect critical infrastructure and citizens from evolving cyber threats with the government's attention and resources focused on cybersecurity.

Secondly, as an official candidate country for EU membership, Albania must align its legal structure with that of the EU and accept the *Acquis Communautaire*, which includes cybersecurity measures. The EU's new cybersecurity approach offers Albania with a roadmap and assistance for aligning its cybersecurity policies and legislation with EU standards. The idea should be that the EU's approach to cyber is the compass that we should use as a country.

Finally, because cybersecurity falls under Cluster 1 on Fundamentals, there is a risk that when Albania receives the green light from Cluster 1 to carry out with the other Clusters, and then returns to Cluster 1 for closure, cybersecurity may cause the closure of the accession negotiations to be delayed.¹⁷³ If the European Union is the aim, the EU's path should be viewed as a road map for Albania to follow.

To begin unravelling the web that is cybersecurity in Albania, the following session will provide an analysis of the legal framework that governs cybersecurity and cyberspace in Albania.

¹⁷¹ According to the open data, AKCESK is the institution with the highest number of growths in the number of employees in 2023, from 24 employees in 2022 to 85 employees in 2023 - an increase with 61 employees, or an increase of 254.17%.

¹⁷² AKCESK, Towards a safe cybersecure ecosystem for Albania. Strategic Vision, 2023. AKCESK (National Authority for Electronic Certification and Cyber Security) as the central authority for the oversight of cybersecurity in country level, increased the number of employees from 24 to 85, and began to explore the possibility to create new monitoring mechanism to identify and respond to cyberattacks.

¹⁷³ "Negotiations on the fundamentals will be opened first and closed last and progress on these will determine the overall pace of negotiations." Enlargement methodology, p 4.



Legal framework

Rather than relying on a single comprehensive cybersecurity regulation, Albania adopts an approach that encompasses laws and regulations that touch upon various aspects of cybersecurity.¹⁷⁴ While these laws provide some level of coverage on issues such as electronic communications, data protection, and electronic signatures, the fragmented legal framework may be challenging for businesses, government agencies, and law enforcement to effectively navigate this complex landscape.

If we view it as an ecosystem, the law that governs cyberspace in Albania is Law No 2/2017 On Cybersecurity.¹⁷⁵ The Law No 2/2017 was adopted as an endeavour to align with Directive 2013/40/EU.¹⁷⁶ The law introduced key institutions of the cyber governance in Albania, such as: The Responsible Authority for Electronic Certification and Cyber Security (AKCESK),¹⁷⁷ Cyber Security Incident Response Team (CSIRT),¹⁷⁸ Important Information Infrastructure Operator and Critical Information Infrastructure Operator, Responsible Minister, and contact points of information, as well as a preliminary outline on how they interact with each-other. This law is currently in force.

This law applies to communication networks and information systems, infringement, or the destruction of which would have an impact on health, safety, economic well-being citizens and the effective functioning of the economy in the Republic of Albania.¹⁷⁹ This law left outside its scope the electronic communications networks and systems information that are object of regulation of the Law on Electronic Signature,¹⁸⁰ Law on electronic identification and trusted services,¹⁸¹ systems that regulate classified information,¹⁸² and networks of electronic communication.¹⁸³¹⁸⁴

¹⁷⁴ <https://cesk.gov.al/wp-content/uploads/2020/07/AlbaniaCMMReport.pdf>, 2018, p 10. Although there is the Law on Cybersecurity which is focussed on cybersecurity, this law mostly deals with the security measures and security related notions of critical information infrastructures and important information infrastructures but does not go in depth on the obligations of the operators of such infrastructures, mechanisms of reporting and duties. These are often regulated by decision of AKCESK or by Decision of Council of Ministers.

¹⁷⁵ Law No 2/2017, On Cybersecurity.

¹⁷⁶ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

¹⁷⁷ The Responsible Authority for Electronic Certification and Cyber Security (AKCESK) in Albania, is the central authority that (a) defines cyber-security measures, (b) acts as the central point of contact at the national level and coordinates tasks for solving cyber security incidents, (c) administers incidents reports, (ç) provides methodical support to operators responsible in the field of cyber security, (d) performs analysis on the weaknesses found in internet, (dh) conducts awareness and education activities in the field of cyber security, and (e) acts as the national Cyber Security Response Team.

¹⁷⁸ Cyber Security Incident Response Team (CSIRTs) are teams made of specialists of the field deployed in every operator of critical information infrastructure and operators of important information infrastructure.

¹⁷⁹ Law No 2/2017, On Cybersecurity, Article 2, para 1.

¹⁸⁰ Law No 9880/2008, On Electronic Signature.

¹⁸¹ Law No 107/2015, On Electronic identification and Trusted Services.

¹⁸² Law No 9457/1999, On Classified Information "state secret".

¹⁸³ Law No 9918/2008, On Electronic Communications.

¹⁸⁴ Law No 2/2017, On Cybersecurity, Article 2, para 2.



This means that the cybersecurity law focuses on certain areas, and the laws excluded by the law govern the aspects that fall outside its scope.

The Electronic and Postal Communications Authority (AKEP) is the designated agency to oversee the implementation of security measures on the undertaking of public electronic communication networks and services in Albania (*playing a similar role as AKCESK*).¹⁸⁵

The case is similar to the National Authority for Information Society (AKSHI). AKSHI administrates every hardware and software system and infrastructure in ICT field, for institutions and budget administration bodies under the responsibility of the Council of Ministers, as well as non-budgetary institutions for which fees will be used the service in Albania.¹⁸⁶ In the event of a security incident involving institutions or state administration entities that fall under the purview of the Council of Ministers, AKSHI coordinates and provides solutions in coordination with the responsible team against computer incidents (CSIRT).¹⁸⁷ The list on the prerogatives of AKSHI is comprehensive. They range from offering IT systems, hardware and ICT infrastructure for governmental entities, to offering services of authentication, electronic signature, and maintaining the hardware and software infrastructure of Albanian, composed of *e-Albania, ICT systems, Register of Online Services, Gov Datacenter, Disaster Recovery Center, Business Continuity Center, Govnet*, to mention a few.¹⁸⁸ Every IT team and system of public institutions or entities of the public administration are administrated by AKSHI; the IT sectors are part of AKSHI structure. Given AKSHI's extensive role in managing ICT infrastructure and services for government entities, it would make sense for AKSHI to take responsibility for ensuring internal compliance with cybersecurity measures set by AKCESK. This internal oversight can include implementing security policies, conducting assessments, and enforcing compliance.

The Law No 2/2017 is expected to be repealed and replaced by the Draft Law on Cybersecurity (or a revised version of the Draft Law), currently on parliament.¹⁸⁹ The Law No 2/2017 provided a narrow overview of the governance model in Albania. The proliferation of recent regulations and laws intertwined with cybersecurity, has created a dismay on who does what in terms of cybersecurity governance in Albania.

According to AKCESK, in the consultation on the revision of the draft law on cybersecurity, it is foreseen that AKEP and AKSHI will take the role of Sectorial

¹⁸⁵ Undertakings of public electronic communications networks and services shall be obliged individually, and jointly where necessary, to adopt appropriate technical and organizational measures to ensure the security of their networks and/or services. AKEP issues a Regulation on the technical and organisational measures/obligations that the operator authorised to provide a network of electronic communication must comply. Regulation No 37, dated 29.10.2015, On technical and organisational measures to guarantee safety and the integrity of communications networks and/or electronic services, Article 6. Operator in the cases of cyber incidents to the information systems, have the obligation to contact and inform AKEP of any infringement or interference in the security or integrity of the communicational network

¹⁸⁶ DCM No 673, dated 22.11.2017, On the reorganisation of National Authority for Information Society, updated, p 1.

¹⁸⁷ *ibid*.

¹⁸⁸ *ibid*, p 4.

¹⁸⁹ Council of Ministers, Draft Law on Cybersecurity.



CSIRTs, which in the current draft law is defined as "the person/team responsible on cyber incidents situated in its relevant sector".¹⁹⁰

The Draft Law on Cybersecurity, does not necessarily address this issue, but it repeals the article that leaves out some information infrastructures outside the scope of the law on cybersecurity, and includes as "other subjects responsible on cyber security" the following entities:

- The responsible authorities on security and defence;
- Ministry responsible for the sector of energy and transport;
- Ministry responsible for the sector for public order and security;
- Ministry responsible for the economy and finance sector;
- Ministry responsible for the health care sector;
- Ministry responsible for environment and territory protection and other related functions;
- Ministry responsible for defence;
- Ministry responsible for agriculture and other related functions;
- National Agency of the Information Society (AKSHI);
- Other institutions responsible for the storage and processing of government data;
- Any other independent public institution that administers information infrastructures in the sense of this law;

and

The entities responsible for providing the services of the following sectors:

- Entities that provide services in the energy sectors, including the electricity, oil gas and nuclear energy sectors;
- Entities that provide services in the air, sea, rail, road and postal transport sectors;
- Entities that provide services in the sectors of the economy, finance, financial market infrastructure, the banking sector, fintech, insurance companies and microfinance systems;
- The state police as a subject with the mission of maintaining order and security public;
- Entities providing services in the healthcare and assistance sectors authorised and accredited by the responsible authorities;
- Entities that provide services in the environmental and protection sectors territory and territorial authorities responsible for supply and distribution of drinking water;
- Entities that provide services in the sectors of digital infrastructure, telecommunications, as well as digital services;
- Entities that provide services in the processing and transmission sectors of classified information related to public security;

¹⁹⁰ Draft Law on Cybersecurity, Article 4.



- Entities that provide services in the academic sector.¹⁹¹

Evidently, the scope has widened significantly. In order to be compliant with the NIS 2 sector in this regard, the law should also foresee the inclusion of:

- Operators of hydrogen production, storage, and transmission;
- Operators of ground-based infrastructure that support the provision of space-based services;
- Undertakings carrying out waste management;
- Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures;
- Food businesses;
- Entities manufacturing medical devices, computer, electronic and optical products, electrical equipment, etc;
- Providers of online marketplaces, online search engines, and social networking services platforms; and
- Research organisations.¹⁹²

Beside the scope, other discrepancies between the Draft Law and the NIS 2 Directive relate to: (1) the definition on who will be considered critical and important information infrastructures and the methodology to choose them¹⁹³, risk assessment and crisis management obligations¹⁹⁴ and sanction regime¹⁹⁵. All these elements in the Draft Law need to be reevaluated in the context of compliance with the NIS 2 directive.

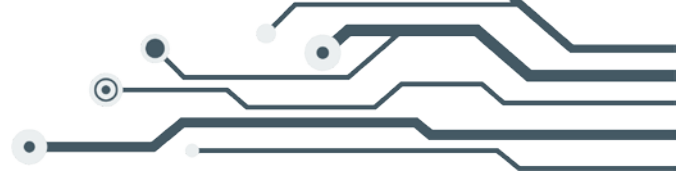
¹⁹¹ Draft Law on Cybersecurity, Article 9.

¹⁹² NIS 2 Directive, Annex 1 and Annex 2.

¹⁹³ CIIOs and IIIOs in Albania will continue to be identified by AKCESK (Article 10/1 Draft Law), which will be done according to a methodology that will be approved by the General Director of AKCESK (Article 10/3 Draft Law). Under the NIS2 Directive, the requirements to adhere to cybersecurity obligations will fall on public or private entities that fulfil certain conditions (Annex 1 of NIS2). In this case, even though Member States and their respective cybersecurity national agencies will send the list of their critical and important infrastructures to the EU bodies, the list will be governed by a set of requirements that will pose obligations directly to the operators of such infrastructures, even if they are not flagged by the National Cybersecurity Authorities, introducing non-compliance fines with a maximum penalty of up to Fines up to 10 million EUR or 2% of the total global annual turnover (whichever is greater) to businesses.

¹⁹⁴ NIS2 Directive applies to all organisations that provide essential services such as health care, energy, transport, water, digital infrastructure, finance, and banking, as well as digital service providers. The innovation of this Directive is that it puts the ball in the field of the CIIOs and IIIOs to take a risk-based approach to cyber security, putting measures in place to protect networks and information systems from cyber-attacks. If not compliant, these operators can face fines with a maximum penalty of up to Fines up to 10 million EUR or 2% of the total global annual turnover (whichever is greater) to businesses (following a similar approach to GDPR).

¹⁹⁵ NIS2 Directive, Article 34, General conditions for imposing administrative fines on essential and important entities.



	NIS 2 Directive	Draft Law on Cybersecurity
The definition on who will be considered critical and important infrastructures and the methodology to choose them	A cap-size rule defined in the Directive. All medium-sized and large entities operating within the sectors or providing services covered by the NIS 2 directive will fall within its scope (Annex)	AKCESK in coordination with other responsible entities on cybersecurity will identify critical and important information infrastructure. The methodology will be approved by the director of AKCKESK.
Risk assessment and crisis management obligations	<ul style="list-style-type: none"> (a) policies on risk analysis and information system security; (b) incident handling; (c) business continuity, such as backup management and disaster recovery, and crisis management; (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures; (g) basic cyber hygiene practices and cybersecurity training; (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption; (i) human resources security, access control policies and asset management; (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. 	<p>1 Operators of critical and important information infrastructure implement technical and organizational measures for risk management, which include measures aimed at:</p> <ul style="list-style-type: none"> (a) Determination of the risk of the incident; (b) Incident prevention, detection and management; (c) Minimizing the effect of the incident; <p>2. During the implementation of organizational and technical measures for risk management, operators take into account especially:</p> <ul style="list-style-type: none"> (a) Security of systems and services; (b) Incident management; (c) Service continuity management; (ç) Monitoring, auditing and testing; (d) Compliance with international standards.
Sanction regime	<p>The NIS2 Directive sets out specific penalties for non-compliance, including:</p> <p>Non-monetary remedies</p>	<p>The fines range from 1 000 000 to 10 000 000 Albanian Lek for not reporting on cyber incidents; 200 000 to 400 000 Albanian Lek for not setting a point of contact and breach of confidentiality; and 400 000 to 1 000 000 Albanian</p>



	<p>Administrative fines</p> <p>Criminal sanctions</p> <p>For essential entities, it requires Member States to provide a maximum fine level of at least €10,000,000 or 2% of the global annual revenue, whichever is higher.</p> <p>For important entities, NIS2 requires Member States to fine for a maximum of at least €7,000,000 or 1,4% of the global annual revenue, whichever is higher.</p>	<p>Lek for not fulfilling the obligations set in the law or by AKCESK.</p>
--	--	--

Table 6: The discrepancies between the NIS 2 Directive and the new Draft Law on Cybersecurity.

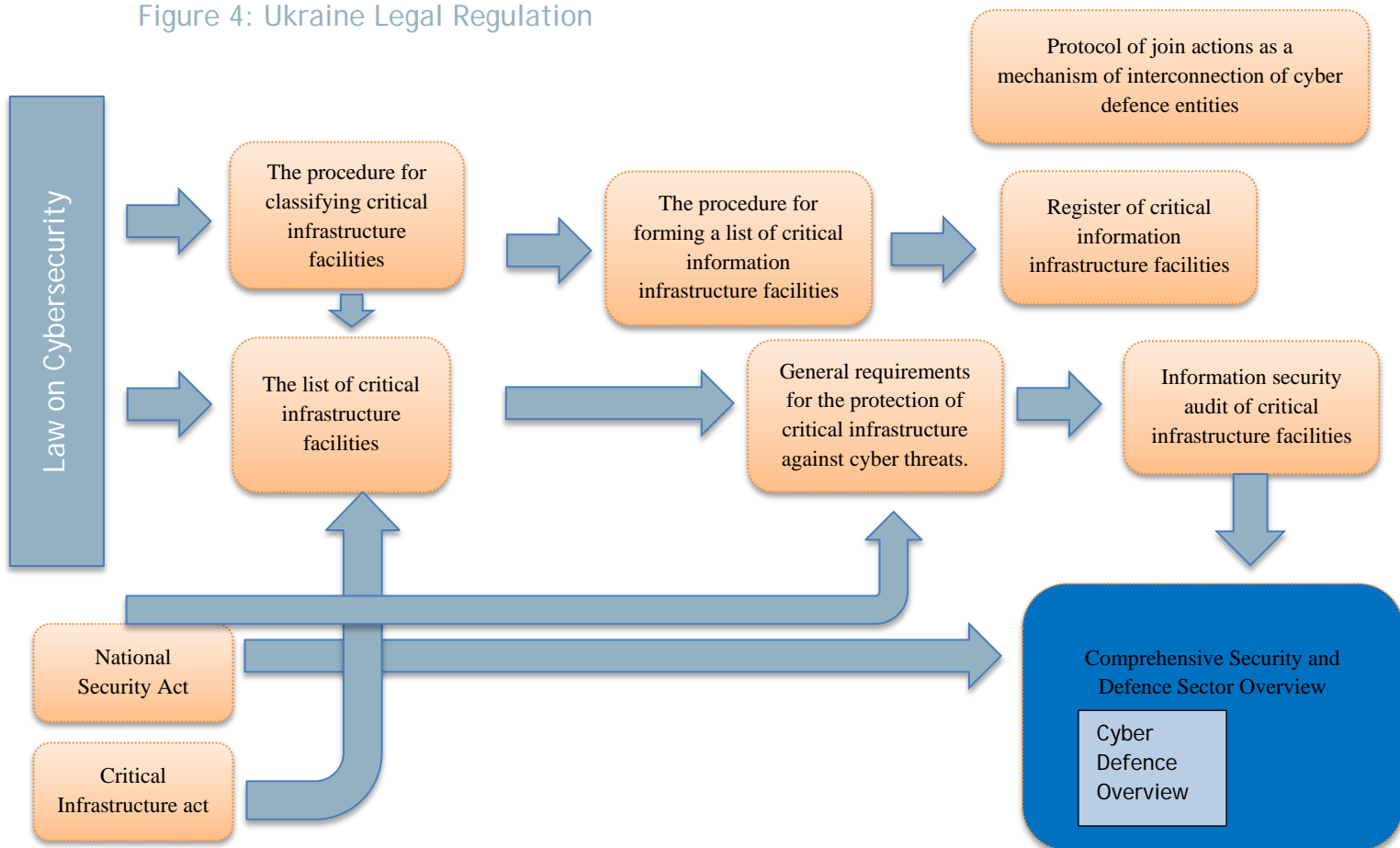
According to AKCESK, in the revised draft law on cybersecurity, a new Methodology¹⁹⁶ will be drafted in compliance with NIS 2 Directive and it shall be applied after the new cyber security law approval. AKCESK notes that Article 12, point 2 of revised the draft law "On cyber security" states that: "The identification of operators of critical and important information infrastructures, according to the definitions made in Annex I and Annex II of this law, is carried out on the basis of a methodology, which is approved by decision of the Council of Ministers."¹⁹⁷

¹⁹⁶ The methodology currently in place is [Metodologjia \(cesk.gov.al\)](https://www.cesk.gov.al/).

¹⁹⁷ Information acquired from consultation with AKCESK.

It would be recommended for the legal framework that governs cybersecurity to clarify certain elements. For instance, Ukraine, which ranks 24th in the National Cyber Security Index.¹⁹⁸, has the following legal regulation on cybersecurity.

Figure 4: Ukraine Legal Regulation



Source: O Bakalynskiy, Case study: major attack on critical infrastructure, CoE. <https://rm.coe.int/ws3-3-cert-ua/168098f6a0>

Albania lacks a Critical Infrastructure Act; and nor the current Law on Cybersecurity or the Draft Law on Cybersecurity contain the procedure for classifying critical infrastructure. Albania has a procedure for classifying critical infrastructure information facilities, which is set in the methodology approved by the Director of AKCESK.¹⁹⁹ However, according to AKCESK, terminology used in the law, "operators of critical and important information infrastructures," is an adapted terminology, aligning with the familiar terminology in the legal and sub-legal acts in force in the Republic of Albania. In the revision of the draft law on cyber security, references are made to its Annexes (I and II), which define critical and important sectors. However, the article itself does not make a specific determination of what qualifies as critical or important. This is because the references to the categorization boundaries of enterprises provided in Annex I of Recommendation 2003/361/EC do not coincide with the boundaries defined in national legislation, namely Law No.

¹⁹⁸ NCSI, Ukraine. <https://ncsi.ega.ee/country/ua/>

¹⁹⁹ Decision No. 9, dated 14.2.2022, Methodology on Identification and Classification of critical and important information infrastructures. <https://cesk.gov.al/wp-content/uploads/2023/09/Metodologjia.pdf>



43/2022, "On the Development of Micro, Small, and Medium Enterprises" (a law that is partially aligned with the relevant EU directive). Consequently, these financial thresholds for classifying medium-sized enterprises as essential or important entities, as defined in the directive, are significantly higher than those defined nationally. Therefore, it becomes impractical to apply this criterion, and the alignment is considered partial. The definitions for the classification of operators of critical and important information infrastructures will be harmonized in the sub-legal acts implementing the new "Cybersecurity Law."²⁰⁰

Nevertheless, the adoption of the abovementioned acts would assist in outlining the roles and responsibilities of government agencies, define national security interests, and establish procedures for responding to security threats, including cyber incidents.

Directive on the resilience of critical entities (CER Directive)²⁰¹ recently adopted on EU level could be a good starting point. If decided to transpose this Directive and enact a law on critical entities, Albania would be obliged to take specific measures aimed at enhancing the resilience of critical entities in two levels: first, to identify critical entities within Albania, and second, to provide support to critical entities in meeting the obligations imposed on them.²⁰² The CER Directive lays down obligations for the Member States to identify critical entities and to support them in meeting obligations imposed on them; and lays down obligations for critical entities as well to enhance their resilience.²⁰³ This overarching approach in imposing obligations to adhere to security in all the levels underpins the new cyber strategy of the EU towards cybersecurity.

Secondly, a strategy on the resilience of critical entities, which would include *"a governance framework to achieve the strategic objective and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties"*²⁰⁴, would solve the uncertainty on the roles and prerogatives of AKCESK, AKSHI, AKEP, Ministry of Defence, National Civil Defense Agency (AKMC) to mention a few.

Thirdly, the CER Directive has foreseen public administration, space, and production, processing and distribution of food as additional sectors as additional sectors that are not foreseen in Albania. Furthermore, the innovation the CER Directive would bring is to define the critical entities based on the following criteria:

- the entity provides one or more essential services;
- the entity operates, and its critical infrastructure is located, on the territory of that Member State; and
- an incident would have significant disruptive effects (...).²⁰⁵

²⁰⁰ In Consultation with AKCESK, regarding the revision of the Draft Law to be compliant with the NIS2 Directive.

²⁰¹ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing council directive 2008/114/EC ('CER').

²⁰² CER, Article 1, para a.

²⁰³ *ibid*, Article 1.

²⁰⁴ *ibid*, Article 4, Strategy on the resilience of critical entities.

²⁰⁵ *ibid*, Article 6.



Meaning, that if an entity fulfils these criteria, the entity as a whole must adhere to the security measures and the obligations set in NIS 2 Directive and CER Directive as well, complimenting each-other in the comprehensive measures.

Since this study focuses on cyber governance and safeguarding critical infrastructures, we won't delve deeply into examining the extent to which the Albanian legal framework aligns with recently adopted regulations like the Digital Operational Resilience Act (DORA)²⁰⁶ and the Cyber Resilience Act (CRA)²⁰⁷, and proposal eIDAS 2.0.²⁰⁸

A note on Law No. 107/2015, "On Electronic Identification and Trusted Services": There is currently a draft law "On Electronic Identification and Trusted Services" in the parliament.²⁰⁹ The draft law aims to be compliant with the Regulation (EU) No. 910/2014 of the European Parliament and of the Council, dated July 23, 2014 "On electronic identification and trust services on electronic transactions in the internal market" (eIDAS).²¹⁰

Excluding the provision that are addressed to member states, the draft law might need to check compliance on the scope and the security provisions of its draft law following the principles of eIDAS2, with the aim to increase the trust of citizens in Albania's digital service providers. The EU is also working in an "EU Toolbox for the European Digital Identity Wallet (EUDI Wallet)", which is considered as "the technical backbone of all future EU Digital Identity wallets, ensuring their safety, interoperability, and user friendliness".²¹¹ Albanian digital service providers and governmental authorities would be encouraged to follow these updates in the EU legal framework, and work towards this standard.

It is highly recommended that Albanian authorities closely monitor and align with the evolving cyber *acquis*, especially given the critical state of accession negotiations. Cybersecurity and alignment with international standards, including those set by the European Union, are paramount for ensuring a smooth and secure transition during the accession process.

Following the legal framework of the country that governs cybersecurity, the next most important thing is the cybersecurity national strategy, which outlines Albania's vision for cybersecurity.

²⁰⁶ Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

²⁰⁷ Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. The main improvements would be the increase of security and reliability in the providers of trust services (*the providers would be obliged to apply the most advances security standards*), increasing cooperation between qualified providers of trust services with state and private institutions, and regulate the legal validity of electronic signatures and seals against the future technological changes.

²⁰⁸ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

²⁰⁹ Draft Law " On Electronic Identification and Trusted Services", Public Consultation, 2022.

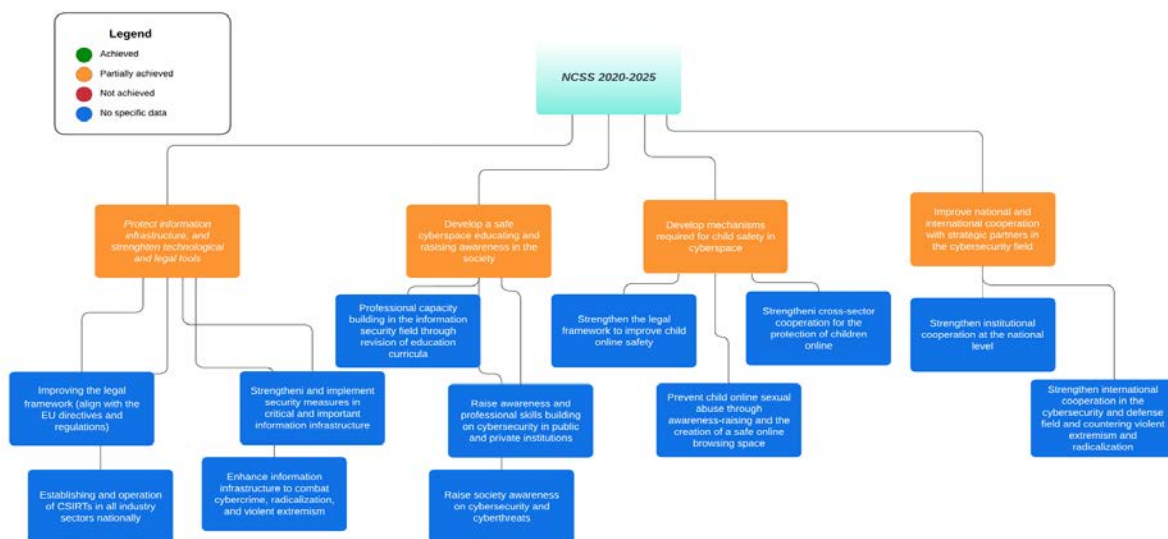
²¹⁰ Monitoring Report on the National Strategy on Cybersecurity 2020-2025, p 6.

²¹¹ EU Digital Identity Wallet Toolbox Process.

Cybersecurity strategy

The main document relating to cybersecurity in Albania is the National Cyber Security Strategy 2020-2025 (NCSS).²¹² The NCSS has 4 policy goals and 14 specific objectives (figure below provides an overview of the NCSS 2020-2025).

Figure 5: Overview of the Albanian National Cyber Security Strategy 2020-2025.



Source: *National Cyber Security Strategy, in conjunction with AKCESK Annual Reports 2020-2022*, [link https://cesk.gov.al/category/raporte/raporte-vjetore/](https://cesk.gov.al/category/raporte/raporte-vjetore/). The link on the report that indicates the level of achievement on each objective is broken, during the date of this study, October 2023

The four policy goals that govern NCSS are:

- **Policy Goal 1:** Protection of information structures and strengthening technological and legal tools;
- **Policy Goal 2:** Awareness raising and education regarding professional capacity building;
- **Policy Goal 3:** Developing mechanisms to ensure child safety in cyberspace; and
- **Policy Goal 4:** Improve national and international cooperation.

²¹² Decision No. 1084, dated 24.12.2020 On adopting the national cybersecurity strategy and its action plan 2020-2025.



The coordinating role to oversee the completion of these goals is AKCESK in cooperation with AKSHI.²¹³

The 2020-2025 National Cybersecurity Strategy (NCSS) includes “improving the legal framework providing norms and regulating cybersecurity in the country and aligning this framework with European Union directives and regulation” as a specified objective.²¹⁴ In line with its National Cyber Security Strategy 2020-2025, Albania recently signed the Second Additional Protocol to the Convention on enhanced cooperation and disclosure of electronic evidence.²¹⁵ As noted above, is also working towards a new Law on Cybersecurity and on adopting sub-legal documents, that aim to align further the legislation framework with the respective EU Directives in the field of security of network and information systems.

As noted in the Strategy, the development of the National Cybersecurity Strategy 2020-2025 is based on the European Union Cybersecurity Strategy.²¹⁶ In order to draw comparison between these two strategic documents, it's essential to delve into the key areas of alignment and divergence, shedding light on how they intersect and where distinctions emerge.

Strategy aspect	EU cybersecurity strategy	Albania National Cyber Security Strategy 2020-2025
Document	The EU's Cybersecurity Strategy for the Digital Decade	Decision No. 1084, dated 24.12.2020 On Adopting the National Cybersecurity Strategy and its Action Plan 2020-2025
Released/signed	16.12.2020	24.12.2020
Key agencies to implement the strategies	EU Agency for Cybersecurity (ENISA)	The National Electronic Certification and Cybersecurity Authority
Agencies' roles	<p>Assist member states in developing cyber-resilience capabilities.</p> <p>Enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes.</p> <p>Cooperates with Member States and EU bodies</p> <p>Examine the feasibility of computer security incident</p>	<p>Defines cyber-security measures.</p> <p>Acts as the central point of contact at the national level for responsible operators in the field of cyber security and coordinates works for resolving cyber security incidents.</p> <p>Administers incident reports in the field of cyber security and ensures the preservation of their registration.</p> <p>Provides help and methodical support to operators responsible in the field of cyber security.</p>

²¹³ National Cybersecurity Strategy, 2020-2025, p 1497.

²¹⁴ National Cyber Security Strategy. Specific Objective 1.

²¹⁵ Council of Europe. News.

²¹⁶ National Cybersecurity Strategy, 2020-2025, p 1496.



	<p>response teams for industrial control systems.</p> <p>share knowledge, developing staff and structures, and raising awareness.</p>	<p>Performs analysis on the weaknesses found in the field of Internet security.</p> <p>Conducts awareness and education activities in the field of cyber security. Acts as the national CSIRT's.</p>
Challenges of the strategy	Adoption of revised NIS Directive (NIS2);	Lack of capacities; the improvement of the overall national cybersecurity situation.
Vision and priorities	<p>Achieve Resilience, technological sovereignty, and leadership.</p> <p>Build operational capacity to prevent, deter and respond - European Cyber Shield & Joint Cyber Unit.</p> <p>Advance a global and open cyberspace.</p> <p>Develop cyber-defence policy and capabilities related to the Common Security and Defence Policy.</p>	<p>Ensure cybersecurity at the national level through the protection of</p> <p>information infrastructure and strengthening technological and legal tools.</p> <p>Develop a safe cyberspace educating and raising awareness in</p> <p>the society regarding professional capacity building in the information security field.</p> <p>Develop mechanisms required for child safety in cyberspace.</p> <p>Improve national and international cooperation with strategic partners in the cybersecurity field.</p>
Key Concern	<p>Possible misalignments on norms for responding to cyber activities below the thresholds relevant under international law.</p> <p>Approving hardware and software, dealing with supply chain dependencies, and managing vulnerabilities.</p>	<p>Too much focus on the legal framework and not enough on problems related to insecure critical and important systems.</p> <p>The enhancement of cybersecurity for structures and entities that fall outside the critical and important infrastructure.</p>

Table 7: Summary of the EU and Albania cybersecurity strategy.

Resilience is an underlying theme and the end-goal of the EUCSS. It focuses more on developing capacities, mechanisms and keeping up with technological advances to increase their security standard. In comparison to Albania's NCSS, it is streamlined on the focus to create a bulletproof (or cyberattack-proof) society. Albania's NCSS remains in a formative stage in developing the cybersecurity legal framework and increasing the capacity in education, safer internet for children and training on cybersecurity. This paper presents the following paradigm:

In this interconnected society, EU Member States government and the Albanian government face a similar threat landscape - 10 terabytes of data are stolen monthly



in the EU.²¹⁷ whereas Albania encounters continuous data leaks;²¹⁸ Distributed Denial of Service (DDoS) attacks rank among the highest threats for EU in general, which is similar to the cyber-attack in 2022 in Albania; the conflict in Russia has mobilised many hacktivists, cybercriminals, and state-sponsored groups.²¹⁹ and the use of social engineering to exploit human behaviour to gain access to information and services is increasing.²²⁰

Based on AKCESK Annual Reports 2020-2022, out of 125 activities foreseen to be completed in the NCSS Action plan, 52% of them are completed in 2021, and 42% are expected to be completed in 2022 and further.²²¹ During 2022, AKCESK has organised trainings specialised to specific sectors, workshops, and conducted reports in cooperation with international partners to provide recommendations and highlight vulnerabilities found in the systems.²²²

However, there is no threat assessment report released by AKCESK (similar ENISA's Threat Landscape report²²³ on the state of the cybersecurity threat landscape), that can provide data on what are the main concerns of Albania's infrastructure vis-à-vis cybersecurity. If these data are found in AKCESK due to the operational tasks of their work, AKCESK would be recommended to thematically prepare reports on different sectors on Albania and provide the data.

In the next section, we will connect the legal rules with how they work in practice, specifically when it comes to making sure our critical and important information infrastructures are resilient and can withstand cyber threats.

²¹⁷ European Council, Infographic - *Top cyber threats in the EU*.

²¹⁸ A2 News Article, US concern, AMP alleges TIMS data leak.


²¹⁹ <https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/>

²²⁰ ENISA, *EU Threat Assessment*.

²²¹ AKCESK *Annual Report, 2022*.

²²² Monitoring Report on the National Strategy on Cybersecurity 2020-2025. <https://cesk.gov.al/wp-content/uploads/2023/07/Raport-Monitorimi-i-SKSK-per-2022.pdf>

²²³ ENISA Threat Landscape (ETL) report.



Cyber resilience and critical infrastructure protection

By definition, critical infrastructures are "systems and assets that are essential for the functioning of a society and economy, and whose disruption or destruction would have a debilitating impact on national security, the economy, public health, safety, or any combination thereof".²²⁴ The Operators of the critical infrastructures inside the jurisdiction of Albania are obliged to implement the requirements of the safety measures given by AKCESK, and to document the implementation of these safety measures.²²⁵ AKCESK determines through a regulation, the content and method of document the safety measures.²²⁶ Article 9 of the Cyber Law provides a list of safety measures, and separates them in two groups: *organisational measures* and *technical measures* to monitor, detect, prevent or mitigate incidents.²²⁷ In the Draft Law on Cybersecurity, it is foreseen that AKCESK will provide with an order the content and the oversight of the fulfilment of the organisational and technical measures.²²⁸

The Critical Infrastructure of Albania is made of all the essential services that underpin the backbone of a nation's economy, security, health, utilities, and transportation and communication systems that the country relies on, on day-to-day basis. An attack or destruction of these vital systems would have a debilitating effect on security, national economic security, national public health or safety, or any combination of such nature. The security of critical infrastructure is of paramount importance since it is essential to the efficient operation and functioning of a nation.²²⁹ Furthermore, secure digital environment is also essential for luring in foreign investment, encouraging innovation, and stimulating economic progress.²³⁰

Critical and Important information infrastructure list are updated at least once in two years, audited by AKCESK at least twice a year. The CIIOs and IIIOs are legal

²²⁴ CISA, *Critical Infrastructure Sectors*.

²²⁵ Article 8, Law 02/2017.

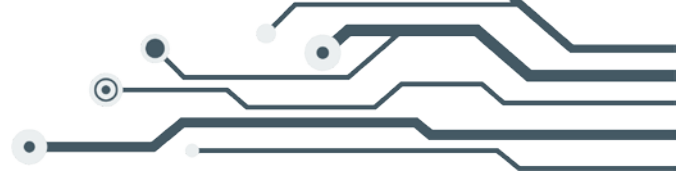
²²⁶ Article 9/3, Law 02/2017.

²²⁷ Organisation measures: information security management, risk management, security policies, organizational security, safety requirements for third parties, dh) asset management, human resources security and people access, security events and management of cyber security incidents, management of work continuity; control and audit. Technical measures are those of: physical security, protecting the integrity of communications networks, verifying user identity, access authorization management, the activity of administrators and users, dh) detection of cyber security events, assets management means of tracking and evaluating cyber security events, application's security, cryptographic equipment, security of industrial systems.

²²⁸ AKCESK, Regulation on the content and method of documenting security measures, approved by the Order No 184, dated 20.07.2023.

²²⁹ European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*.

²³⁰ UNCTAD, *World Investment Report 2023*. For instance, industries struggling with supply chain challenges, including electronics, semiconductors, automotive and machinery, saw a surge in projects, while investment in digital economy sectors slowed.



entities, private or public, that administer Critical Information Infrastructure²³¹ and Important Information Infrastructure.²³² AKCESK is the central authority, tasked with the duty to identify the operators - public sector operators, government sector infrastructures and identification of critical and important information infrastructure in the private sector.

As noted, operators are required to report information related to incidents or potential incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to AKCESK.²³³ AKCESK determines by regulation the types and categories of cybersecurity incidents, as well as the format and elements of the cybersecurity incident report.²³⁴ In the case of cybersecurity incident and attacks on constitutional, security and defence institutions, AKCESK reports immediately to the leaders of these institution on the issues and measures to be taken.²³⁵ Furthermore, AKCESK is the authority that has the power to fine the CIIOs and IIIOs in the cases where they violate provisions of the Law on Cybersecurity (in particular related to the omission of cyber incidents, failure of certain obligation, not updating the Authority on point of contact and other relevant information, and failure within duties of corrective measures).²³⁶

Notably, a new fundamental change that NIS2 has brought is the new rule on what can be classified as critical and important infrastructure. Currently in Albania, the list of CIIOs and IIIOs is proposed by AKCESK and approved by the Council of Ministers. Below is an overview of the entities that are considered as critical information infrastructures and important information infrastructure.

²³¹ Critical Information Infrastructure is the entirety of networks and systems information, the violation or destruction of which would have a serious impact on health, security and/or economic well-being of citizens and/or the effective functioning of economy in the Republic of Albania.

²³² Important Information Infrastructure is the entirety of networks and systems owned by a public authority, which is not part of the critical infrastructure of information, but that could jeopardise or limit the work of the public administration in the event of information security breaches.

²³³ Law 02/2017 On Cybersecurity.

²³⁴ Law 02/2017 On Cybersecurity.

²³⁵ Law 02/2017 On Cybersecurity. Article 22.

²³⁶ Law "On Cybersecurity", Article 21.



Sector	Critical Information Infrastructure Operators		Important Information Infrastructure Operators	
	Private Sector	Public Sector	Private Sector	Public Sector
Energy	○ 6 CIIs Operators ²³⁷	-	○ 4 IIIs Operators	-
Transport	○ 8 CIIs Operators ²³⁸	-	○ 5 IIIs Operators	-
Banking	○ 13 CIIs Operators ²³⁹	-	○ 7 IIIs Operators	-
Financial services	○ 5 CIIs Operators ²⁴⁰	-	○ 18 IIIs Operators	-
Healthcare and Public Health	○ 13 CIIs Operators ²⁴¹	○ 1 CII Operator - Ministry of Health and Social Protection	○ 7 IIIs Operators	-
Water supply	○ 6 CIIs Operators ²⁴²	-	○ 37 IIIs Operators	-
Digital infrastructure	○ 2 CIIs Operators ²⁴³	○ 19 CIIs Operators ²⁴⁴	-	○ 11 IIIs Operators

Table 8: Critical Information Infrastructure Operators and Important Information Infrastructure Operators

If we focus on the cyber resilience of the critical infrastructures in Albania, one of the key gaps of the Law No 2/2017 On Cybersecurity is that it fails to specify on what

²³⁷ Operatori i Shpërndarjes së Energjisë Elektrike, Operatori i Sistemit të Transmetimit, Korporata Elektroenergjetike Shqiptare, Kurum International sh.a., Dragobia Energy Prell Energy, sh.p.k. Power Elektrik Slabinje, Seka Hydropower shpk, Devoll Hydropower sha, Trans Adriatic Pipeline (TAP).

²³⁸ Albcontrol sh.a., Tirana International Airport, Kukës International Airport Zayed, Autoriteti Portual Durrës, Porti Detar sh.a. Sarandë, Porti Detar Shëngjin, Drejtoria e Pergjithshme e Sherbimit te Transportit Rrugor, Posta Shqiptare sh.a..

²³⁹ Banka e Shqipërisë, Intesa San Paolo Bank – Shqipëri, Banka Kombëtare Tregtare, OTP Bank Albania, Alpha Bank, Banka e Bashkuar e Shqipërisë, Union Bank, Raiffeisen Bank sh.a, Banka e Parë e Investimeve. Banka Credins, Banka Tirana ProCredit Bank, Banka Amerikane e Investimeve sh.a..

²⁴⁰ SHKK “FED invest”, IuteCredit, Crimson Finance Fund Albania, sh.p.k., Kredo Finance, Fondi Besa sh.a..

²⁴¹ American Hospital & International Hospital, Liv Hospital Tirana, 3P Life Logistic, Klinika Kajo, Ana Diagnostic Center, Noval Diagnostic, Intermedica, Marketing & Distribution Salus Pegasus Med, Fondacioni “Klinika Orthodokse e Ungjilhezimit”, Laboratory Networks shpk.

²⁴² Shkodër sh.a., UK; Tiranë sh.a., UK; Durrës sh.a. UK; Elbasan sh.a., UK; Vlorë sh.a., UK; Fier sh.a., UK.

²⁴³ Shkodër sh.a., UK; Tiranë sh.a., UK; Durrës sh.a. UK; Elbasan sh.a., UK; Vlorë sh.a., UK; Fier sh.a., UK.

²⁴⁴ Ministry of Defence, Agjencia e Zhvillimit të Territorit, Agjencia Kombëtare e Shoqërisë së Informacionit, Instituti i Sigurimeve Shoqërore, Drejtoria e Përgjithshme e Tatimeve, Drejtoria e Përgjithshme e Pronësisë Industriale, Agjencia Shtetërore e Kadastres, Qendra e Shërbimeve Arsimore, Qendra Kombëtare e Biznesit, Drejtoria e Përgjithshme e Gjendjes Civile, Agjencia e Prokurimit Publik, Drejtoria e Pergjithshme e Burgjeve, Ministria e Infrastruktues dhe Energjise, Departamenti i Administrates Publike, Drejtoria e Pergjithshme e Standartizimit, Drejtoria e Pergjithshme e Doganave, Ministry of Justice, KLGJ.



are the obligations for ensuring cybersecurity for CIIOs and IIIIOs. If we compare this law with the Cybersecurity Act, dated on 09.05.2018 of Estonia (*not aligned with the NIS2 Directive yet as well*).²⁴⁵ is that the later lays down the obligations for service provider.²⁴⁶ (in the Albanian law meaning CIIOs and IIIIOs) to ensure the cybersecurity of their network and information system, the basis for notifications of incidents, the criteria of cyber incidents with a significant impact and the tasks of the Information System Authority (in our case - AKCESK) in coordinating cybersecurity and organising cross-border co-operation. In the Albanian Law "On Cybersecurity", it is noted that "The [CIIOs] and [IIIIOs] are required to report to the Authority **immediately** after detecting cyber security incidents"²⁴⁷, whereas the Estonian Cybersecurity Act has it clearly defined that "A service provider shall inform the Estonian Information System Authority immediately but no later than **24 hours** after becoming aware of a cyber incident".²⁴⁸

To further illustrate, CIIOs and IIIIOs need to understand their obligations and security measures and comply with the by-laws written by AKCESK or check DCM that provide the *technical* and *organisational security* measures. The regulation adopted by AKCESK.²⁴⁹ does do not construe the same level of blanket obligations as set in the Estonian Cybersecurity Act. However, AKCESK notes that in the new cyber law, there will be a clear list of the obligations of CIIOs and IIOs, in full compliance with NIS 2 Directive.²⁵⁰

AKCESK needs to continue monitoring on Critical Infrastructures and Important Infrastructures, to check their implementation of security measures, through (not informed) penetration testing and ad hoc audits. AKCESK has foreseen six events in the last trimester of 2023, comprised of a TTX and CyberDrill, each directed to a particular sector, in health, energy, transport, finance, water supply and banking.²⁵¹ AKCESK is recommended to include a research team into these trainings, as well as to publish the findings on the level of preparation of the sectors to the public.

In the Annual Report of AKCESK 2022, it is noted that AKCESK has audited with the method (onsite) 6 CIIOs (*out of 73 CIIOs*) and 5 IIIIOs (*out of 89 IIIIOs*), on the implementation of the basic minimum-security requirements.²⁵² Meaning, that in one year, AKCESK has audited only 8% of CIIOs and 6% of IIIIOs in the implementation of security measures issued by AKCESK. In terms of evaluating the security of CIIs and IIIs Operators on their emergent security measures, AKCESK has audited 42 CIIs Operators (out of 73 CIIs - 57%) and 29 IIIs Operators (out of 89 IIIs Operators - 32%) in 2022,²⁵³ which is a better outcome. In 2022, AKCESK conducted a risk assessment

²⁴⁵ Cybersecurity Act of Republic of Estonia dated 09.05.2018.

²⁴⁶ *ibid*, Chapter 2 Obligations for ensuring cybersecurity.

²⁴⁷ Law On Cybersecurity, Article 11, para 1.

²⁴⁸ Cybersecurity Act, Chapter 2, § 8.

²⁴⁹ Regulation on the content and method of documenting measures of cybersecurity, amended by the Order No. 184, dated on 20.07.2023.

²⁵⁰ Information acquired in consultation with AKCESK.

²⁵¹ AKCESK, events <https://cesk.gov.al/en/events-2/>.

²⁵² AKCESK, Annual Report 2022, p 12.

²⁵³ *ibid*, p 16.



on the institutions related to security and defence.²⁵⁴ It would be highly valuable that these data be made to the public for research and transparency reasons.

AKCESK needs to increase the number of audits on CIIOs and IIIOs in the implementation of organisational and technical measures. The lack of oversight could potentially result in non-compliance. In the revised draft law, AKCESK notes that the fine regime will go to 1.000.000 to 10.000.000 ALL in case of breach of the provisions of the law.²⁵⁵

However, there is no information whether the inclusion of "or the 7-10% of the annual turnover" is included in the law.

As cybercriminals continue to evolve their tactics and techniques, governments must improve their cybersecurity capabilities, invest in advanced threat detection technologies, and promote a culture of cyber awareness among the public officials' employees.²⁵⁶ Strengthening cybersecurity frameworks, conducting frequent audits, and adopting proactive monitoring systems are critical steps towards strengthening defence mechanisms and mitigating cyber incursion threats. Furthermore, international cooperation in sharing information, intelligence, and best practices is critical to effectively combating the global character of cyber threats.²⁵⁷

For example, the 2022 in Albania cyber-attack on did not occur in a vacuum. Over the course of 2022 and 2023, four Western Balkan (WB) countries, namely Albania, Kosovo, North Macedonia, and Montenegro, experienced a wave of cyberattacks.²⁵⁸ The *modus operandi* of the cyber criminals was consistent across all four WB countries. The cybercriminals would target state institutions with ransomware, DDoS, and phishing attacks to bring the country's digital infrastructure down.

In the background of Russia-Ukraine war²⁵⁹, concerns are raised over the Western Balkans, particularly in regard to a NATO report stating that it has "observed cyberattacks, disinformation, intimidation and other destabilizing activities in the Western Balkans in the past 12 months."²⁶⁰ The cyberattacks of 2022 are assumed to be connected to Russia, as Russia, as quoted by the North Macedonia President

²⁵⁴ *ibid*, p 14.

²⁵⁵ Information acquired in consultation with AKCESK.

²⁵⁶ Metamorphosis, A recent look towards Cybersecurity in the Western Balkans: How can we improve the cybersecurity level in the region?. <https://metamorphosis.org.mk/en/blog/a-recent-look-towards-cybersecurity-in-the-western-balkans-how-can-we-improve-the-cybersecurity-level-in-the-region>. According to AKCESK Annual Reports, AKCESK has been actively engaged in conducting trainings, workshop, cyber drills - however, it would be a good standpoint to incorporate an outside standard to measure the impact of these activities to the general cyber architecture of Albania.

²⁵⁷ UNODC, International cooperation on cybersecurity matters.

²⁵⁸ Metamorphosis.

²⁵⁹ ANKASAM, Western Balkan Countries' Intelligence Capabilities Under the Looming Shadow of Increasing Cyberattacks, 8 October 2022. <https://www.ankasam.org/western-balkan-countries-intelligence-capabilities-under-the-looming-shadow-of-increasing-cyberattacks/?lang=en>

²⁶⁰ CNBC, One year on, Russia's war in Ukraine ramps up fears over Europe's next security 'soft spot', 20 February 2023. <https://www.cnbc.com/2023/02/20/russia-ukraine-war-stokes-security-fears-in-the-western-balkans.html>



Pendarovski considers "[the Western Balkans] as the so-called soft spot in the whole pan-European security architecture right now, apart from Ukraine of course".²⁶¹

Based on a possible chance that this premise is true, Albania needs to work on its resilience of critical infrastructure, government institutions or businesses against the efforts of criminal organisations, hacktivists groups, or individual hackers, with the intent to gain unauthorised access to sensitive data, disrupt services, or compromise privacy for a pay/gain. Furthermore, given the dynamic threat environment, which includes evolving terrorist and hybrid threats as well as rising infrastructural and sectoral interdependence, more needs to be done to adequately equip such institutions.

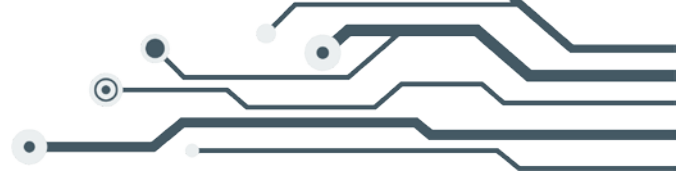
Increasing international cooperation in the field of cybersecurity with strategic partners is a policy goal of the National Cyber Security Strategy and a priority for AKCESK which has signed cooperation agreements/memorandums of understanding with different countries. These documents can be accessed in this link: [Marrëveshje Bashkëpunimi](#) - AKCESK. Albania is a member of different international organizations and forums. In the field of cyber security, it cooperates with the UN, OSCE, NATO, EU (ENISA), GFCE, DCAF, Council of Europe, FIRST, FESA, Trusted Introducer, etc. In addition, NAECCS of Albania cooperates with different countries, allies and partners, such as the United States of America, United Arab Emirates, Israel, Romania, North Macedonia, etc. Cooperation with neighbouring countries has been strengthened. Regarding information sharing and capacity building, AKCESK plays an active role in the UN, NATO, and OSCE. AKCESK notes that they continuously work on enhancing its international cooperation with the aim of coordinating efforts to implement international cyber security standards and policies based on best practices and guarantee a secure cyberspace.²⁶²

Recognizing the shared challenges and the need for a united response, regional cooperation is critical in effectively combating cyber threats. Under the regional cooperation framework in the Western Balkans, the six countries need to explore the idea to establish, or if established, make use of mechanisms for timely information sharing, intelligence collaboration, and joint response actions.²⁶³ This approach can help to identify common vulnerabilities, understand emerging cyber threats, and develop robust defence strategies that consider regional dynamics. As all the countries in the WB aspire to join the European Union, they need to start reflecting their alignment with the EU's plan to strengthen its cyber resilience and promote cyber security cooperation in the region.

²⁶¹ *ibid*

²⁶² Information acquired in consultation with AKCESK.

²⁶³ Regional Cooperation Council, SEE2030 Strategy. <https://www.rcc.int/see2030/files/SEE-2030-strategy.pdf>



National cybersecurity governance

There is no document in Albania that lists the organisations involved in the security architecture, their organisational structure, and their responsibilities. Based on the fragmented regulations, we understand the following on the cybersecurity governance framework in Albania.

As noted through this paper, **AKCESK** is the central authority responsible for the overall national cybersecurity measures and overseeing the enforcement of laws on electronic signatures, electronic identification, trusted services, and cybersecurity. Its mission is *“the achievement of a high level of cyber security, by defining security measures, rights, obligations and the cooperation of subjects that work in the field of cybersecurity”*.²⁶⁴ It also acts as the national CSIRT.²⁶⁵, meaning the authority is the official national coordinating body for the reporting and management of cybersecurity incidents for the Important information infrastructures and critical information infrastructures operators.²⁶⁶

AKCESK is the main point of contact in cases of attacks and incidents and is the key institution responsible for the implementation of the National Cybersecurity Strategy and its Action Plan.

AKCESK also plays the role of the **National CIRT**. The AL-CIRT structure is responsible for the detection and management of potential cyber threats that could pose risks to the Republic of Albania. It is actively engaged in responding to cybersecurity incidents and implementing necessary measures to mitigate their impact. Additionally, AL-CIRT leverages insights gained from past incidents to enhance its preparedness for future cybersecurity challenges, strengthening the protection of critical systems and data in Albania. This mechanism also addresses any legal issues that may arise during incidents. Furthermore, it actively promotes the exchange of knowledge among its constituents and disseminates valuable security best practices and guidance through various channels, including publications, websites, and other communication mediums.²⁶⁷

If we compare AKCESK to ENISA or other cyber security organisations in the EU, AKCESK lacks publication of guidelines and studies to support critical infrastructure in increasing their resilience against cyber-attacks. In the Monitoring Report on the National Cyber Security Strategy 2020-2025 and AKCESK Annual Reports, it is noted that AKCESK draft reports and protocols on different sectors. To reiterate, comparing to ENISA, who continuously publishes guidelines and studies to authorities in increasing their resilience against cyber-attacks.²⁶⁸, AKCESK lacks this approach as there are no reports (outside the scope of its work), assessment or guidelines easily

²⁶⁴ Law 02/2017 On Cybersecurity, Article 5.

²⁶⁵ *ibid*

²⁶⁶ See generally AKCESK, Rregullore e Brendshme. <https://cesk.gov.al/wp-content/uploads/2020/07/Rregullore-e-Brendshme.pdf>

²⁶⁷ AKCESK, Work methodology. <https://cesk.gov.al/wp-content/uploads/2023/06/Udhezim-per-Metodologjine-e-punes-detyrat-qe-duhet-te-zbatojne-CSIRT-et-ne-nivel-Kombetar.pdf>

²⁶⁸ ENISA.



accessed in their webpages. Entities outside the scope of the list of critical and important entities could benefit from these guidelines.

In EU Member State level, the Information System Authority, the equivalent of AKCESK in Estonia, publishes comprehensive assessment on the state of cybersecurity in Estonia annually amidst other publications.²⁶⁹ AKCESK needs to reflect on this good practice. For instance, in this research, a detailed reporting on the state of cyber security in Albania in the last five years would prove to be immensely beneficial. The Albanian citizens, business and operators of important and critical information infrastructures would see the benefit in these reports as well.

AKSHI is the agency under the authority of the Prime Minister's office which is specialised on *e-government* and *information society*. AKSHI is responsible for administering and maintaining e-governance services, e-taxation, e-procurement, e-customs, eDriving license etc.²⁷⁰ AKSHI is also responsible for administering ICT systems of public institutions and is the key institution with regards to the drafting and implementation of the Digital Agenda Strategy.²⁷¹ It ensures safe authentication and identification, safe internet and DNS for the public administration in the services that it provides at the Government Data Centre. AKSHI is the authority in charge of supervision of the implementation of the law on electronic signature and law on e-governance, and sublegal enactments issued in accordance with these laws. Therefore, if AKCESK is the responsible authority to audit CIIIs and IIIs on the implementation and documentation of security measures, AKSHI has this role for the digital services providers and the trusted service provider that fall within the e-governance scope. AKSHI itself is under the supervision of AKCESK, as AKSHI is classified as a CIII.

According to Law No 43/2023 On Electronic governance, AKSHI is the responsible authority on electronic governance, and the central governmental infrastructure.²⁷² Under the new law, AKSHI has a threefold role: (1) as a service provider, (2) creator, developer and administrator of systems and infrastructures; and (3) as a contributor to the drafting of policies in the ICT field. AKSHI in governing and creating the infrastructure of electronic governance must oversee and provide for continuous systematic protection and security of e-government infrastructure in compliance with safety regulations.²⁷³

AKEP is an **independent** regulatory body that oversees electronic communications and postal services and has the authority to issue administrative sanctions in cases of violation. AKEP can request Internet Service Providers (ISPs) to remove illegal content based on the decisions of the competent authorities. It supervises, checks, and monitors the activity of the providers of the electronic communication networks and electronic communication services, and also supervises the implementation of

²⁶⁹Information System Authority.

²⁷⁰ Akshi.gov.al

²⁷¹ DCAF, Cybersecurity And Human Rights In The Western Balkans: Mapping Governance And Actors. <https://www.dcaf.ch/cybersecurity-and-human-rights-western-balkans-mapping-governance-and-actors>

²⁷² Law No 43/2023 On Electronic Governance, Article 22.

²⁷³ *ibid*, Article 8.



the necessary measures taken by the providers for the security and integrity of public electronic communications services and networks regarding the protection of personal data. AKEP also manages the .al country code. Different from AKSHI and AKCESK, AKEP is an independent body. Like AKCESK and AKSHI, AKEP is the authority responsible for auditing the implementation and documentation of security measures of the service providers under their scope of work. Meanwhile, AKEP itself is under the supervision of AKCESK, for being classified as a CIII.

AKCESK, AKSHI, AKEP and other critical infrastructure and important infrastructures, among other stakeholders, need to refer cases of data breaches, criminal offences related to computer crimes and other possible interferences with the system to the competent authorities to investigate these. There is the [Albanian State Police C-Unit](#) for all the region of Albania²⁷⁴ and the [Prosecutor's Cybercrime Investigation Unit](#) which can investigate and exercise criminal prosecution against cybercrimes in these instances.

[The Ministry of Defence \(MoD\)](#) is the responsible ministry for handling the MoD and Air Force related cyber-incidents and oversees the implementation of the National Strategy for Cyber Protection²⁷⁵. In the NCSI Index, Albania has received a score of zero in the category 12.1 "*Cyber operations unit*", lacking these requirements (i) *Military forces have a unit (cyber command, etc.) that is specialised in planning and conducting cyber operations;* (ii) *Military forces have conducted a cyber operations exercise or an exercise with a cyber operations component in the country in the last 3 years,* (iii) *Military forces have conducted a cyber operations exercise or an exercise with a cyber operations component in the country in the last 3 years,* and (iv) *Military forces have conducted a cyber operations exercise or an exercise with a cyber operations component in the country in the last 3 years.*²⁷⁶

An overall score of zero in this category does affect the rank of Albania as 54th in the National Cyber Security Index.

In June 2023, NATO-EU task force created with the purpose of making critical infrastructure, technology and supply chains more resilient in the face of continuously evolving threats and risks, published their final assessment report.²⁷⁷ The reports notes that "*Disruptions to critical infrastructure can have significant negative consequences for vital government functions, essential services to the population and economic activity in Allies and Member States. They can also hamper military activities, including exercises, deployment, reinforcement and sustainment. Moreover, complex interdependencies mean that a disruption to critical infrastructure can have cascading or mutually reinforcing effects.*"²⁷⁸ NATO-EU Task Force has identified four sectors as providing services that support and enable other sectors: energy, transport, digital infrastructure and space, protection

²⁷⁴ As noted above, cybercrime falls outside the scope of this paper, however, the author would want to highlight the issue with Albanian citizens obligation to come to Tirana to report a cybercrime, even if their residence is in Tropojë, Sarandë or Permet, as an alerting point.

²⁷⁵ MoD, [Strategy on Cyber Defence 2021-2023](#).

²⁷⁶ NCSI, Albania.

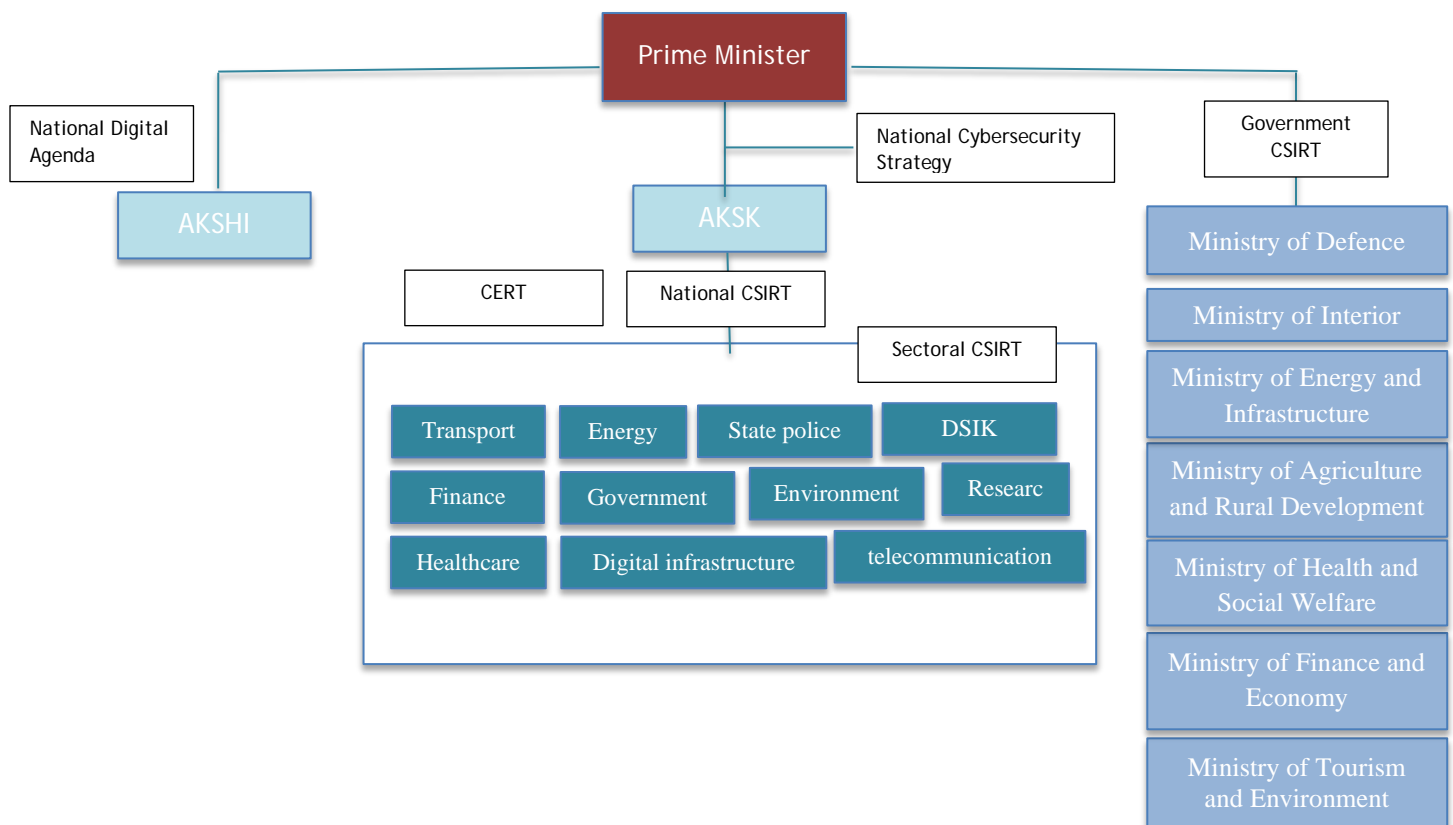
²⁷⁷ EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report.

²⁷⁸ *ibid*, p 3.

of which require tailored measures to ensure resilience, and calls for allies (Albania included) and Member States to enhance "their preparedness to confront disruptions to critical infrastructure".²⁷⁹ As we understand, these developments underscore the significance of strengthening Albania's cybersecurity and critical infrastructure resilience to effectively counter evolving threats and ensure the security and stability of critical and important information infrastructures.

The Draft Law on Cybersecurity has proposed the following model on cyber governance.

Figure 6: Albanian cybersecurity governance



AKCESK is rebranded as the National Authority for Cyber Security (AKSK). AKSK continues to be the responsible authority for general coordination of cybersecurity policy. AKSK will identify and classify critical and important information infrastructures based on a methodology approved by the Director of AKSK.²⁸⁰ Differently from the previous model, AKSK will be under the authority of the Prime Minister office.

In order to resolve cyber events, AKSK will serve as a focal point on the national and international levels and coordinate the responsibilities with other institutions responsible for cybersecurity. The list of institutions in Albania responsible for cybersecurity has been enlarged to include ministries of critical sectors, AKSHI,

²⁷⁹ *ibid*, p 8.

²⁸⁰ Draft Law on Cybersecurity, Article 10.



entities that administer information infrastructures, and critical sector operators as outlined in this draft law.²⁸¹

The explicit assertion of AKSK's duties and obligations, both as the national authority for cyber security and as the National CSIRT, is a positive element introduced in the Draft Law on Cybersecurity.

Operators of essential and important information infrastructures must have a person or team responsible for responding to cyber incidents in their information infrastructure (Operator CSIRT) as well as a sectorial CSIRT for the operator's relevant sector.²⁸² In a gist, the Sectoral CSIRT coordinates with the National CSIRT to increase the level of cybersecurity in the critical and important information infrastructures, whereas the Operator CSIRT monitors the networks and information systems of the operator in case of a possible cyber-attack, among other things.²⁸³

In the case of a cyber crises, an ad hoc structure is created by AKSK in coordination with other subjects responsible for cybersecurity, responsible for the management of the cyber emergency - CERT. CERT is composed of 10 experts called by AKSK to draft emergency plans, management and provide solutions to the emergency.²⁸⁴ Furthermore, AKSK's development and administration of a National Security Operations Centre (SOC) is an important step forward in Albania's cybersecurity infrastructure. A SOC is an essential component of a nation's cybersecurity strategy, and the establishment of one by AKSK demonstrates the country's commitment to improving its cybersecurity capabilities.²⁸⁵ It should be noted that such centres have already been established prior to the adoption of the Draft Law on Cybersecurity.²⁸⁶

Overall, the exercise of defining cyber governance in Albania is complex. The Draft Law on Cybersecurity mentions the concept of cyber governance only one time, when noting the obligation of the operator of a critical information to have a team of at least 3 people, requiring one of them to be trained in cyber security governance.²⁸⁷ This notion is not mentioned in any other legal act, nor explained in detail in the Draft Law on Cybersecurity. The fragmented nature of cybersecurity governance in Albania highlights the need for a more comprehensive and integrated approach to address the country's cyber governance challenges effectively.

²⁸¹ *ibid*, Article 9.

²⁸² *ibid*, Article 13.

²⁸³ *ibid*, Article 13 and 14.

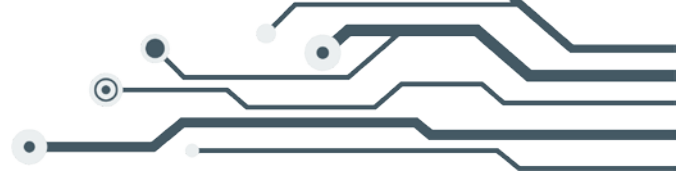
²⁸⁴ *ibid*, Article 24.

²⁸⁵ *ibid*, Article 8. A Security Operations Centre (SOC) is a command center for cybersecurity professionals responsible for monitoring, analysing, and protecting an organization from cyber-attacks. In the SOC, internet traffic, internal network infrastructure, desktops, servers, endpoint devices, databases, applications, IoT devices, and other systems are continuously monitored for security incidents. The SOC staff may work with other teams or departments but are typically self-contained with employees that have distinguished cybersecurity skills. Most SOC's operate 24-7 with employees working in shifts to monitor network activity continually and mitigate threats.

²⁸⁶ Edi Rama, 'Qendra Operacionale e Sigurisë Kibernetike (AKCESK)'.

<https://www.youtube.com/watch?v=irINeAAMpNs>

²⁸⁷ Draft Law on Cybersecurity, Article 14, para 2.



For example, the model of cyber governance of Italy is far more comprehensive than the current model followed by Albania. In Italy, the prime minister is the highest authority of the cybersecurity and is supported by an *Inter-Ministerial Committee for the Security of the Republic* [CISR] (composed of the Ministry of Foreign Affairs, the Ministry of Interior Affairs, the Ministry of Justice, the Ministry of Defence, the Ministry of Economy and Finance, and the Ministry of Economic Development).²⁸⁸ This Inter-Ministerial Committee has an advisory role, but it also develops and adopts new strategies related to the national cyber security framework.²⁸⁹ A *Technical Committee for the Security of the Republic* (T-CSISR) supports the CISR in implementing correctly the cybersecurity national plan.²⁹⁰ In Italy, the Security and Intelligence Department (DIS), which coordinates all intelligence activities including cybersecurity, serves also as a link to manage the relationships with EU, NATO, OSCE, and the UN.²⁹¹ The equivalent to AKCESK/AKSK in Italy is the Cyber Security Unit (NCS), which is an interagency and intergovernmental operational body "responsible for preventing and preparing for a national cyber crisis, for declaring such a crisis, and for coordinating the responses by competent bodies following the Prime Minister's decisions".²⁹² NCS is chaired by a Deputy Director General from the DIS and made up of a Military Advisor and representatives from the Intelligence Department and from the Ministries of Foreign Affairs, Interior, Justice, Economic Development, Economy and Finance and the Department of Civil Protection.²⁹³ Italy has a National CERT (CERT-N), which is part of the Ministry of Economics and Development; a Public Administration CERT; and a dedicated entity overseeing the protection of national critical infrastructure against cyber-attack, called the National Anti-Crime Centre for the Protection of Critical Infrastructure.²⁹⁴ Italy also has a military command exclusively in charge of conducting cyber operations, the Joint Cyber Command. Schematically, Italy cybersecurity landscape can be represented as below:

²⁸⁸ S Colarin, 'National Cybersecurity Organisation: ITALY (CCDCOE)', p 13.

https://ccdcoe.org/uploads/2020/04/NCS_organisation_ITA_2_0_FINAL.pdf

²⁸⁹ *ibid.*

²⁹⁰ *ibid.*

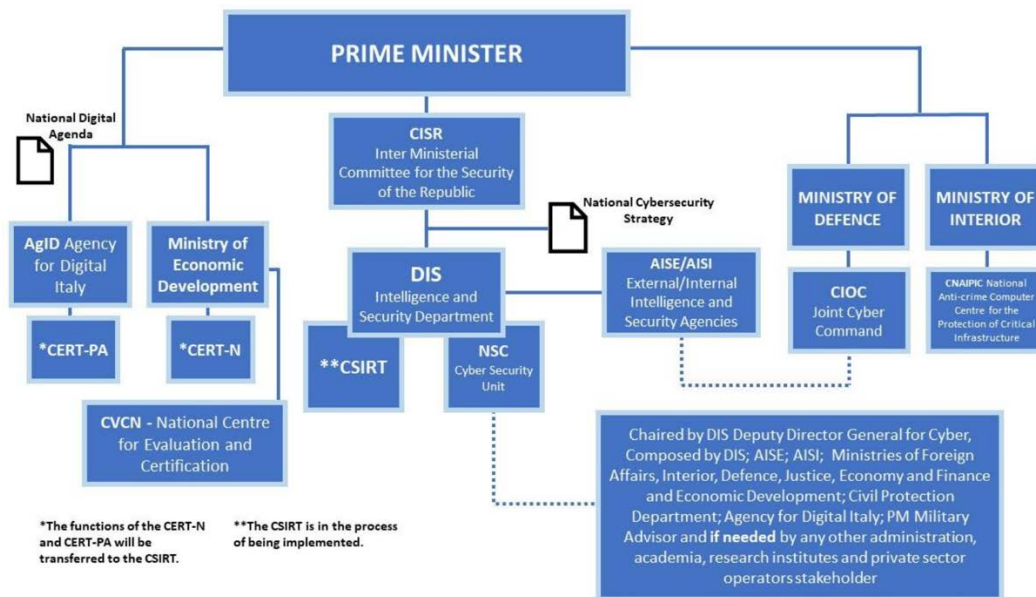
²⁹¹ *ibid.*

²⁹² *ibid.*, p 14.

²⁹³ *ibid.*

²⁹⁴ *ibid.*, p 16.

Figure 7: Italian cybersecurity architecture



Source: CCDCOE, *National Cybersecurity Organisation: ITALY*.
https://ccdcoe.org/uploads/2020/04/NCS_organisation_ITA_2_0_FINAL.pdf

Albania follows a completely different approach to Italy, and the reason behind this is not clearly understood. Almost all the functioning of the abovementioned institutions falls under the scope of AKCESK/AKSK in Albania. AKCESK is the authority to draft cybersecurity regulation, to oversee the implementation of organisational and technical security measures from CIIOs and IIIOs, to keep contact and coordinate in cases of cyber crises both national and international, and to run 24/7 SOC's.

Albania follows a different model compared to Estonia as well. In Estonia, the Ministry of Economic Affairs and Communications is the responsible authority for the general coordination of cybersecurity policy.²⁹⁵ The Cyber Security Council of the Government Security Committee, made of seven ministries and the government office, supports cross-departmental strategic cooperation and monitors the implementation of the cybersecurity strategy.²⁹⁶ The Estonian Information System Authority mentioned briefly above, the equivalent to AKCESK, is responsible for the development and management of the government's information systems, coordinating the implementation of security standards, and drafting policies and strategies.²⁹⁷ Differently from Italy and similarly to Albania, the Estonian Computer Emergency Response Team (CERT-EE) is located within the RIA. However, different from Albania, the national computer security incident response capacity is

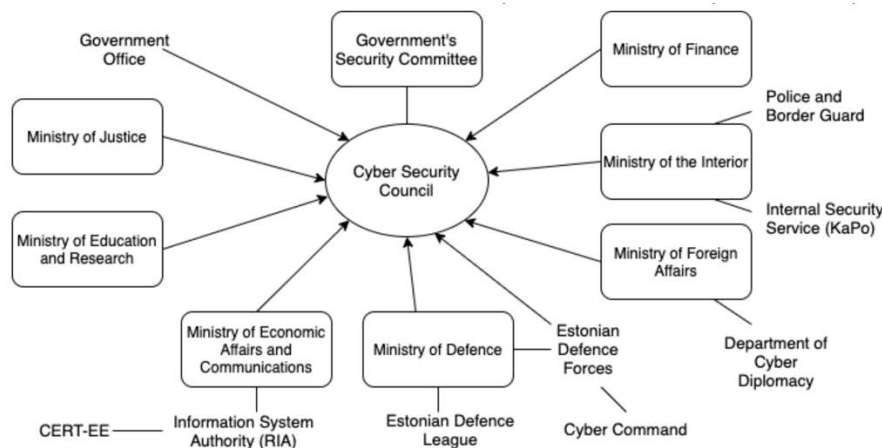
²⁹⁵ K Kohlre, 'Estonia's National Cybersecurity and Cyberdefense Posture', p 9.
https://www.researchgate.net/publication/344351180_Estonia's_National_Cybersecurity_and_Cyberdefense_Posture

²⁹⁶ *ibid.*

²⁹⁷ *ibid.*

operational 24/7.²⁹⁸ In Estonia, the Ministry of Defence is responsible for cyber defence as part of the national defence.²⁹⁹ Besides the Ministry of Defence, national cyber defence is supported by the Estonian Defence League's Cyber Defence Unit (EDL CDU), which includes cybersecurity professionals from both public and private entities.³⁰⁰

Figure 8: Composition of the Cyber Security Council of the Government Security Committee in Estonia.



Source: K Kohler, *Estonia's National Cybersecurity and Cyberdefense Posture*, (2020).

https://www.researchgate.net/publication/344351180_Estonia's_National_Cybersecurity_and_Cyberdefense_Posture

Subsequent to this discussion on Albanian cyber landscape, the following priority tasks are suggested to be considered by national authorities:

Draft a whitebook on the role and impact of cybersecurity in Albania, how critical infrastructures interact with each-other, impacts of cyber-attacks on critical infrastructure to the country, technologies to protect (IoT, Cloud, Wireless communication and 5G) to mention a few. A report that should be a true reflection of the state of cybersecurity, cyber governance and cyber resilience in Albania

Draft legislation in accordance with the Critical Entities Resilience Directive (CER).³⁰¹ The conundrum on what is considered critical infrastructure or not needs to be regulated in law, rather than by decision of a public official. In today's interconnected world, a sector which is *de facto* critical, but *de jure* no, would compromise the security of the national infrastructure in its entirety.

²⁹⁸ *ibid.*

²⁹⁹ *ibid.*

³⁰⁰ *ibid.*, p 10. The Estonian Defence League is a volunteer defence organisation with approximately 16,000 members. The Estonian Defence League Act of 2013 formally incorporates the EDL CDU into the national defence system, providing a framework for its formation, management, membership, and operation (see Baezner, 2020).

³⁰¹ The Directive (EU) 2022/2557.



Either define the cybergovernance model in Albania in a legal act, setting clear roles, responsibilities, and interactions between stakeholders, or include such element in the next National Cyber Security Governance. In conducting this exercise, the national authorities need to consider the best practices on EU and international level. At the moment, we are clear how AKCESK interacts with CIIOs and IIOs, and Prime Minister, however, considering the complicated cyber architecture in different countries, this simple approach could prove to be ineffective against cyber threats.

Reduce and narrow the scope of AKCESK's responsibilities to exclusively cover cybersecurity and introduce new organizational structures to become integral parts of Albania's cyber governance framework.




The dilemma

According to our research of the EU cyber landscape, we understand that EU is throwing a long ball even for the capacities of its Member States. They have, however, opted to take a "forward-looking approach" to the digital age. The thesis question - the problem - that has motivated this work is whether Albania should catch up with the new EU norm, in the process of changing its trajectory, or whether it should maintain the initial position set prior to the EU's revised attitude.

It should be underlined that not every initiative taken by the EU should be followed by the Albanian government a priori, without first determining if the initiative is content specific, EU specific, or if it is even applicable to Albania in the current conditions. However, from a policy point of view, the EU's measures are not isolated, but rather part of a worldwide strategy to cybersecurity.³⁰² This would suffice us to understand that this is the future standard where the global society is heading towards. In the context of Albania, we must consider two scenarios that could develop if we do not align our cybersecurity landscape with that of the European Union.

³⁰² EU Cyber Direct. EU, UK, Japan Comparison. <https://eucyberdirect.eu/>



Scenario 1: Lagging in Cybersecurity advancement.

The dilemma is raised on whether the parliament should choose to adopt the Draft Law moulded under the old model or amend the draft law in compliance with the new NIS2 Directive requirements, with the aim to be *on a par* with EU member states. In our viewpoint, the NIS2 Directive introduces a number of requirements that would be beneficial to the Albanian society, like (i) *carrying out regular risk assessments of information and communication systems (ICS)*; (ii) *taking appropriate measures to mitigate the risks identified in the risk assessments; reporting all significant cybersecurity incidents to the national cybersecurity authority (NCA) within 24 hours*; (iii) *notifying customers of any significant cybersecurity incidents that are likely to have a negative impact on their services; and cooperating with the NCA in the investigation of cybersecurity incidents.*³⁰³ Moreover, NIS2 puts on a series of obligations for critical entities, including specific requirements for third-party risk management that CIIOs and IIIOs operators that want to join the EU digital market need to comply.³⁰⁴ Vice-versa, investors, companies, and even EU-entities and agencies that would want to conduct business in Albania, will most probably ask for guarantees on cybersecurity measures taken from the counterpart. Saying this, AKCESK would need to oversee CIIOs and IIIOs and ascertain whether they have the capabilities to prevent, detect, and respond to cyberattacks on the EU standard.

Furthermore, on the draft law report, it is noted that the approval of the draft law will bring financial effects for the state budget, since the law foresees the establishment of the National Cyber Security Centre, the establishment and implementation of standards, as well as continuous training of the Authority's staff in order to increase capacities. Also, this draft law brings financial effects for CIIOs and IIIOs related to the investments that must be made to strengthen security measures for the protection of their information systems and networks.³⁰⁵ If this law is not fully compliant with NIS 2 Directive (notwithstanding the provisions closely related to being a Member State), the law will most definitely be amended in the next two years, due to the obligations part of the accession negotiations. This is costly to the budget of the state. For this reason, the parliament needs to make a budgetary analysis in addition to a capacity analysis, to determine whether Albanian authorities can comply with the NIS 2 Directive at the current state.

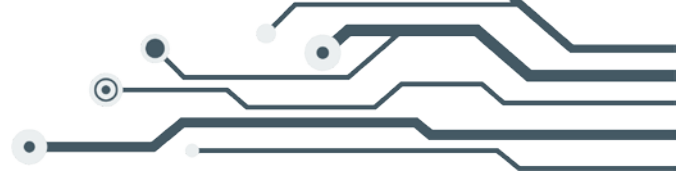
However, the Albanian legislation needs to comprehend that the underlying theme in most of the new EU regulations and directives is the investment in new technologies, and security standards that operators of the critical infrastructures and important infrastructures need to comply with.³⁰⁶ In the case that entities and critical infrastructures residing in Albania do not have the legal requirement to

³⁰³ NIS2 Directive.

³⁰⁴ NIS2 Directive, para 88, p 17.

³⁰⁵ Draft Law on Cybersecurity, Report, p 8. <https://konsultimipublik.gov.al/Konsultime/Detaje/626>

³⁰⁶ European Commission, 'Digital Europe Programme', <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>



comply with the best standards to protect these infrastructures, it is reasonable to presume that Albania cyber infrastructure will lag in comparison to its EU counterparts. This is not important only for a comparison level on where the Albanian infrastructure stand in terms of cybersecurity *vis-à-vis* the European ones. The issue with a discrepancy in cybersecurity compliance level will most probably be an issue for future cooperation between EU-Albania investments and cooperation, based on the logic of the supply chain attack. Due to a possibility that cybercriminals that seeks to damage EU, will aim to target less secure elements in the supply chain, the EU entities will not jeopardise their security by collaborating with a less secure, or a not strong-security adhering entity.

Furthermore, EU's new approach to cybersecurity reflects the evolving nature of cyber threats and the adoption of more sophisticated measures to counter them. By sticking with the past cyber framework, Albania risk missing out the latest cybersecurity advancements and best practices that are continuously being developed by the EU. This could result in a lack of preparedness to address emerging cyber threats effectively and may leave Albania vulnerable to cyberattacks.



Scenario 2: Incapability with EU standards

In the context of Albania's aspirations for EU membership, cybersecurity is a key component within the framework of the Accession Negotiations process. This scenario, often referred to as "Incapability with EU Standards", emphasises the importance to align its cybersecurity practises with the standard set forth by the EU.

Cybersecurity falls within the First Cluster of the Accession Negotiations process³⁰⁷, which includes a variety of policy areas and legislation that candidate nations like Albania must align with the EU. In this context, "incapability" suggests that Albania currently, or consequently from this decision, would lack the requisite infrastructure, legislative frameworks, or cybersecurity capabilities to completely meet the EU's cybersecurity requirements. As a result, for Albania to move forward in its EU accession process, it must focus on closing the cybersecurity gap between its current capabilities and the EU's stringent cybersecurity standards.

Moreover, given the focus it is given momentarily to increasing cyber resilience, and particularly now, as Albania and other EU Candidate countries, can apply for the calls of funding of the Digital Europe Programme³⁰⁸ which has an overall budget of €7.5 billion in the 2021-2027 period, aiming to catch the EU in its shift of trajectory not only be a wise course of action, but it would also demonstrate Albania's readiness to join the EU.

³⁰⁷ <https://cluster1albania.com/>

³⁰⁸ European Commission, 'Digital Europe Programme', <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>



Conclusion

The European Union has taken a proactive and comprehensive approach to cyber security, including various elements, such as the creation of operational centres for the monitoring of cyber-attacks, cyber diplomacy, cyber defence, the creation of networks for the exchange of information and cooperation among many elements of others, signal the very nature of cyber security.

The decision is closely linked to the development of malicious tools to attack critical and important infrastructures of countries. The development of new technologies, as well as the interdependence of the country with technology, has caused the countries, including the European Union, to be in a state of alert on the establishment of cyber security as a priority. This is logical, since almost every sector of a country, be it health, education, defence, energy, transport, or space, operates based on technology. Furthermore, these infrastructures are interconnected. A problem in the energy sector, such as an attack that disrupts the operation of the electrical distribution network, can lead to doctors in hospitals unable to operate on patients, factories left without power to produce, planes unable to fly for because they don't have the computers to navigate the airspace, and a series of unfortunate events that follow one moment: a cyber-attack on an operator of a critical infrastructure in the energy sector.

This paper presented a comprehensive examination of the strategic, institutional, and legal framework for cybersecurity in Albania. In order to assess Albania's alignment with the European Union in the field of cybersecurity, it examined the cyber landscapes of the EU, Albania, and EU vs Albania in terms of certain features and identified areas of misalignment.

A wrongful reflection on the state of cybersecurity and cyber defence in the country could lead in a problematic state of unawareness to the level of vulnerability. Since cyber policy discourse in Albania is not quite developed, the paper scope was to focus on cybersecurity in Albania expansively, rather than thoroughly. The author agrees that every finding and point raised in this paper necessitates its own study, with the purpose to further clarify the cyber landscape in the country.

For this reason, the role of AKCESK, as well as other actors in Albania, is seen as key to being more proactive and connected to a common challenge. Despite the existence of a level of coordination between AKCESK, CSIRTs, sectoral CSIRTs, the study calls for more research on what cyber governance model would work best for Albania.

In this context, Albania is positioned in two standpoints: firstly, since Albania is in a digitisation process, both of public services, but also of critical and important information infrastructures, cyber-attacks can bring substantial damage, up to in a paralysis of the state to function properly. For this reason, following the best practices, both in terms of the legal, regulatory and technical framework, is very important, both at the state level, but also at the operator level. On the other hand, Albania is in the process of joining the European Union. This membership is accompanied by a list of requirements, which Albania must not fulfil only as long as



it becomes part of the EU but are continuous obligations that every member state must comply with.

Even if the Albanian government can argue that there is currently no infrastructure to meet the new EU requirements, if the EU is our ultimate objective, then such an infrastructure will exist at some point as a legal obligation.

To conclude, resolving the dilemma is not an easy task. Even if the Albanian government argues that there is now no infrastructure in place to meet the new EU requirements, if the EU is our final target, then such infrastructure must eventually exist. It should be emphasised that Albania is dedicated to harmonising its cybersecurity legislation with EU standards, as evidenced by the main areas of alignment in e-governance electronic signatures, cybersecurity fulfilling minimal requirements in line with NIS 1 Directive, and electronic communications. To ensure Albania's cybersecurity readiness and advance its larger goal of European integration, it is imperative to address the outstanding challenges and achieve full compliance with EU requirements.



Recommendations

To the Parliament:

The Parliament is recommended to consider the evolving EU acquis in the field of cybersecurity when consulting the adoption of the draft laws currently in parliament. This proactive approach will help prevent discrepancies between Albania and the EU, fostering cooperation and investment opportunities while effectively countering cyber threats. Moreover, any new or revised cybersecurity legislation should include clear and detailed obligations for CIIOs and IIIOs, to be compliant with the NIS2 Directive. These obligations should encompass risk assessment, incident reporting, and compliance with specific cybersecurity measures.

At this moment in the negotiation process for membership in the European Union, the adoption of laws with partial compliance with the EU acquis can be considered as a temporary solution, which requires a considerable budget to implement, and then, to be reviewed at a second time (except in cases where partial compliance is related to the impossibility of fulfilling legal obligations closely related to being a member state). As far as possible, for the protection of one of the basic principles of a state, such as legal certainty, the Albanian parliament is recommended to ensure that the law that is being asked to be approved will not have changes (or be completely repealed), in the foreseeable future. In the cases discussed in this study, it is estimated that the draft law on cyber security lacks some essential elements of the NIS 2 Directive, which may lead to a revision of this law in the short term. The Parliament is recommended that the new law on cyber security should be compliant at the highest level that the lack of status as a member state of the European Union allows.

For this reason, and particularly related to the field of cybersecurity, the parliament is recommended that all the draft laws related to ICT, and the governing cyber legal framework, be in full compliance (as far as compliant a candidate country can be without the status of a member country) with the following EU *acquis*:

The Critical Entities Resilience Directive (CER) [Directive (EU) 2022/2557], which calls for the country to adopt a strategy for the resilience of critical entities and ensure that critical entities take appropriate and proportionate technical and organisational measures to ensure their resilience. The EU has adopted this Directive to complement the NIS 2 Directive. Albania lacks a legislation regulating critical entities at this level.

Digital Operational Resilience Act (DORA) [EU Regulation] that sets down obligations on financial institutions to follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

Proposals Cyber Resilience Act (CRA) that focuses on targeting security of digital things since the design of the products; and eIDAS 2.0, that will lay down the standard on the digital identification and authentication framework.



There draft law "On Electronic Identification and Trusted Services" falls under the same dilemma as this paper. Although eIDAS 2.0 Regulation is yet to be adopted, if adopted, it will foresee a different regulation that the Regulation (EU) No. 910/2014 of the European Parliament and of the Council, dated July 23, 2014 "On electronic identification and trust services on electronic transactions in the internal market" (eIDAS). The parliament needs to assure that the budget, time, and resources of the country will go towards sustainable laws.

To the Government:

The EU is focusing on enhancing the resilience of the critical infrastructures at EU level and Member State level, through new obligations and measures that need to be taken by essential entities and government. For this reason, the PM is recommended to recognise cybersecurity as a national priority and integrate it into broader national security and digital transformation strategies.

Embracing the Digital Operational Resilience Act (DORA) proposal to establish uniform cybersecurity requirements for organisations in the financial sector and critical third-party service providers, the government is recommended to invest in securing the digital identities of Albanian citizens by supporting initiatives like the European Digital Identity Wallet (EUDI Wallet). In working towards the EU standard, meaning that the digital identities will be secure, reliable, and compliant with EU regulations, this will be a checked box when Albania heads to Cluster 3.

A recommendation is to increase investment in cybersecurity research, cyber assessments, workforce development, and emerging technologies to bolster Albania's cyber resilience. Albania currently does not have any cyber risk assessment that could provide insights on the level of vulnerability against cyber threats, or areas that are most critical to focus.

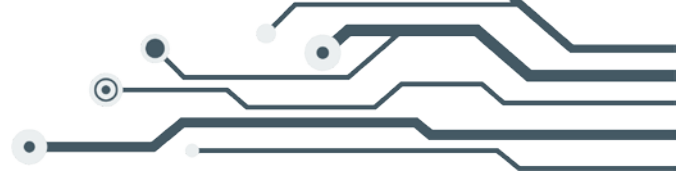
Consider implementing specific regulations for critical infrastructure in Albania, akin to the EU's regulations, to provide clarity and guidance to Critical Information Infrastructure Operators (CIIOs) and Important Information Infrastructure Operators (IIIOs).

The government is recommended to define the cyber governance model in Albania. AKCESK interacts with Critical and Important Infrastructure Operators either through contact points, or through established CSIRTs, which are operational-technical groups focused on cyber security. Other models followed in Europe foresee a more cooperation and coordination led model between different stakeholders.

Encourage collaboration between government entities, private sector organizations, and academia to share threat intelligence, best practices, and resources for improving cybersecurity. Establish public-private partnerships to enhance the security of critical infrastructure.

To Ministry of Defence:

To address the deficiency highlighted in the NCSI Index, Albania needs to establish a dedicated cyber operations unit within its military forces. This unit needs to be responsible for planning and conducting cyber operations, conducting regular



exercises, and developing the skills and expertise necessary to defend against cyber threats.

Develop and regularly update incident response and recovery plans for both cyber and physical incidents affecting critical infrastructure. These plans need to involve coordination among relevant stakeholders and include strategies for minimizing downtime and damage.

It is recommended to carry out exercises and training within the personnel regarding the use of the cyber diplomacy toolbox, to improve cooperation and coordination against malicious cyber activities.

It is recommended to continue the promotion of civil-military cooperation, emphasising that the cooperation in the cyber domain is based on the exchange of best practices, information, and cooperation with the civilian CSIRT network.

To AKCESK:

AKCESK needs to strengthen its oversight role in monitoring and enforcing cybersecurity measures among CIIOs and IIIOs. This includes conducting regular audits and assessments to ensure compliance with cybersecurity requirements.

A recommendation is to invest in making AKCESK a hub for stakeholders to go to get guidance and support on cybersecurity risk management, incident response, and best practices. AKCESK could explore the possibility of developing clear guidelines and standards tailored to the specific needs of critical infrastructure sectors in Albania.

Develop a Blueprint for coordinated response to major cyber-attacks, aligning it with the EU blueprint for effective crisis management.

Provide regular reports and updates on the state of cybersecurity in Albania to the government, relevant authorities, and the people. The lack of report and research on Albania's state of vulnerability is a concern that should be addressed. In addition to annual reports and weekly newsletters, reports on challenges, vulnerabilities, as well as the most vulnerable sectors to cyber security in Albania would be added value to increase awareness of the country's overall cyber security.

AKCESK, as the institution responsible for coordinating work on cyber security and for drafting the National Strategy for Cyber Security (based on the draft law on Cyber Security), is recommended to include a model of cyber governance in Albania, based on the requirements of the Nis 2 Directive (Article 7/c), to clarify the roles and responsibilities of the relevant subjects at the national level.

To CIIOs and IIIOs:

Although Albania is not yet an EU member state country, and the new standard introduced by the EU could be considered as stringent to the operations of CIIOs and IIIOs, the operators of the critical and important information infrastructures are recommended to proactively begin the compliance with the new standards, as a test run when these requirements will come into power. The sanctions introduced in the



NIS2 Directive could be detrimental to their operations. Moreover, these obligations will arise if CIIOs and IIIOs will engage in business with essential entities in the EU. For this reason, these recommendations are given to CIIOs and IIIOs, based on the new EU standard on cyber resilience and cybersecurity:

- Conduct regular risk assessments to identify vulnerabilities in your information systems, and develop comprehensive incident response plans to effectively address cybersecurity incidents and minimize potential damage;
- Invest in cybersecurity training programs for your employees to enhance their awareness and skills;
- Prioritise data protection and privacy by implementing strong encryption, access controls, and data handling procedures;
- Have in place policies on risk analysis, system security and Incident handling; and
- Use Multi-Factor Authentication (MFA) and secure emergency communications.



Annex 1 - Terminology

Communication network and information system: an electronic communications network, or any connected or interconnected equipment or set, of which one or more that one, based on a program, perform automatic data processing; or digital data stored, processed, found or transmitted for the purpose of operation, use, protection and maintenance.

Critical Information Infrastructure Operator: a legal person, public or private sector, which administers critical information infrastructure

Critical Information Infrastructure: the entirety of networks and systems information, the

Critical Infrastructure: systems and assets that are essential for the functioning of a society and economy, and whose disruption or destruction would have a debilitating impact on national security, the economy, public health, safety, or any combination thereof.

CSIRT: the Computer Security Incident Response Team.

Cyber espionage: the covert and unauthorized activity of infiltrating computer systems, networks, or devices to gather sensitive or classified information, trade secrets, intellectual property, or other valuable data for the purpose of espionage, intelligence gathering, or economic advantage.

Cyber Incident: a Cyber security event during which there is a violation of the security of services or information systems and networks communication and brings a real negative effect.

Cyber Resilience: an organization's ability to withstand, adapt to, and rapidly recover from cyberattacks, data breaches, or any form of security incidents.

Cyber Security Risk: a circumstance or event, identifiable in reasonable way, which can cause the security of the service or security information systems and communication networks.

Cyber Security: consists of practices and methods for securing data, information, and integrity of various components of cyberspace, including but not limited to the physical aspects of the medium.

Cyber Space: the digital environment capable of creating, processing and processing exchange information generated by systems, information society services, as well and electronic communication networks.

Cyber Threat: a potential incident or event that could compromise the confidentiality, integrity, or availability of computer systems, networks, data, or digital assets.



Cyber warfare: the use of digital technology, including computer systems, networks, and software, to conduct aggressive or hostile actions in cyberspace with the intent of causing harm, disruption, or damage to an adversary.

Cyber governance: the framework, policies, procedures, and practices that organizations and governments implement to manage and oversee their cybersecurity activities.

Data breaches: a security incident where an unauthorized individual or entity gains access to sensitive, confidential, or protected information, resulting in the exposure, theft, or compromise of that data.

Digital Infrastructure: the hardware, software, networks, data centres, and communication systems that support various digital services, applications, and information flow.

Distributed denial-of-service (DDoS) attacks: malicious attempts to disrupt the regular functioning of a network, service, or website by overwhelming it with a flood of traffic or requests.

Electronic Signature: any data in electronic form which is attached to or logically associated with other data in electronic form and which is used as a way of verifying the signer's identity and the authenticity of the signed document.

Hacking: an attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely.

Important Information Infrastructure Operator: a legal entity public, which administers important information infrastructure.

Important Information Infrastructure: the entirety of networks and systems information owned by a public authority, which is not part of the critical infrastructure of information, but that could jeopardize or limit the work of the administration public in the event of information security breaches.

IoT device: a physical object or gadget that is connected to the internet and capable of collecting, transmitting, and receiving data.

Malware: any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.

Ransomware attacks: a type of malicious cyberattack in which hackers encrypt a victim's data or computer systems and demand a ransom to provide the decryption key.

SCADA - Supervisory Control and Data Acquisition: is a computer system for gathering and analysing real time data. These systems are used to monitor and control industrial plants or equipment.



References

Albanian legislation:

- Law No. 2/2017, "On Cybersecurity".
- Law No. 107/2015, dated 1.1.2015 "On Electronic Identification and Trusted Services" (as amended).
- Law No. 9880/2008, dated 25.2.2008, "On Electronic Signature" (as amended).
- Law No. 10273, dated 29.4.2010 "On Electronic Document" (as amended).
- Draft Law "On Cybersecurity".
- DCM No. 553, dated 15.7.2020 "On the approval of the list of critical information infrastructures and the list of important information infrastructures", (Amended by VKM No. 761, dated 12.12.2022) (Attachment attached to AKCESK).
- DCM No. 1084, dated 24.12.2020, "On the approval of the National Cyber Security Strategy and Action Plan 2020-2025".
- DCM No. 141, dated 22.2.2017, "On the organization and operation of the National Authority for Electronic Certification and Cyber Security".
- DCM No. 553, dated 15.07.2020, "On the approval of the List of Critical Information Infrastructures and the List of Important Information Infrastructures".
- DCM No. 495, dated 13.9.2017 "On the approval of the rules for the benefit of public electronic services".
- DCM No. 69, dated 27.1.2016, "On the approval of the regulation "On Electronic Identification and Trusted Services".
- DCM No. 973, dated 2.12.2015 "On the approval of the policy document for cyber security 2015-2017".
- DCM No. 357, dated 24.4.2013 "On the approval of the regulation on DE Management"
- Regulation on the content and manner of documenting security measures (Version 2.0) (Amended by Order No. 148, dated 20.07.2023).
- AKCESK, Memorandum of Understanding list.
- Internal Regulation on the organization and operation of the National Authority for Electronic Certification and Cyber Security (Approved by Order of the Prime Minister, no. 87, dated 1.07.2020).
- Regulation on Categories of Cyber Incidents as well as the format and elements of the report (Approved by order no. 62, dated 10.09.2018).
- Guidelines for the Methodology of the Organization and Operation of CSIRTs at the National Level (Approved by order no. 55, dated 31.07.2018).

EU acquis:

- 1st EU Cybersecurity Strategy (EUCSS)
- 2nd Cybersecurity Strategy (EUCSS)



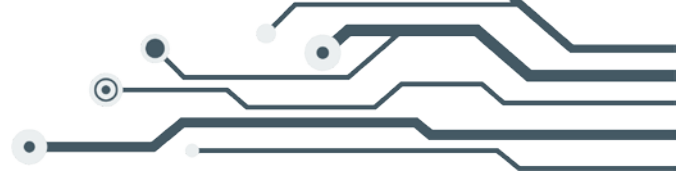
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). [ECI Directive]
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the “NIS Directive”).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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).
- Directive (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

Studies

- Colatin S, National Cybersecurity Organisation: ITALY (CCDCOE), (2020).
- Dutton W, Creese S, Esteve-González P, Goldsmith P, Harris M, Carolin H, Next Steps for the EU: Building on the Paris Call and EU Cybersecurity Strategy, (2022).
- Falessi N, Gavriila R, Klejnstrup M, Moulinos K, National Cyber Security Strategies. Practical Guide on Development and Execution, ENISA (2012).
- K Kohlre, Estonia's National Cybersecurity and Cyberdefense Posture, (2020).
- OSCE, Cyber Incident Classification: A report on emerging trends within the OSCE Region, (2022).
- Papakonstantinou V, Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?, Elsevier, Computer Law and Security Review 44 (2022) 105653.
- Papanikos G, The European Union’s recovery Plan: A Critical Evaluation, (2020)

Reports

- “ENISA Threat Landscape 2021” EU Agency for Cybersecurity.
- “NCSC Annual Review 2021” National Cyber Security Centre.



- “How a European Cyber Resilience Act Will Help Protect Europe” European Commission.
- “The European Union, Cybersecurity, and the Financial Sector: A Primer” Carnegie Endowment for International Peace.
- “GDPR Enforcement Tracker” CMS.
- “Strengthening EU-wide Cybersecurity and Resilience — Council Agrees Its Position” European Council.
- “Cyber Resilience Strategy Changes You Should Know in the EU’s Digital Decade” Security Intelligence.
- “EU negotiators agree on strengthening Europe’s cybersecurity” European Commission Press Release.
- “Proposal for a European Cybersecurity Competence Network and Centre” European Commission.

Websites

- European Digital SME Alliance. <https://www.digitalsme.eu/cybersecurity-label/>.
- NCSI, National Cyber Security Index. <https://ncsi.ega.ee/ncsi-index/>.
- ITU, Global Cybersecurity Index 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
- The Global Economy, Security threats index. https://www.theglobaleconomy.com/rankings/security_threats_index/.
- EuRepoC, [Cyber Incidents](#).
- EU Sanctions Map, Sanctions Map. <http://www.sanctionsmap.eu/>.
- World Economic Forum, Global Security Outlook 2023. <https://www.weforum.org/reports/global-cybersecurity-outlook-2023>
- Cluster1Albania. <https://cluster1albania.com/>
- Kryeministria. Kryeministria.al
- AKCESK. <https://cesk.gov.al>
- AKSHI. <https://akshi.gov.al/>

