THE IMPORTANCE OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION – CASE OF ALBANIA

KLORENTA PASHAJ[1], ERALDA GJIKA[2], LULE BASHA[3]

[1]National Authority for Cyber Security of Albania, Directorate of Monitoring and Incident Response, Operations Center SOC C-SIRT

[2,3]Department of Applied Mathematics, Faculty of Natural Science, University of Tirana

e-mail: klorenta.pashaj@gmail.com

Abstract

Since the inception of the internet, protecting critical information infrastructure has been essential, particularly as attacks on such systems increasingly impact all vital sectors. This protection is a collective responsibility shared between the public and private sectors. In Albania, the National Authority for Cyber Security (NACS) serves as the national Cyber Incident Response Team (CSIRT), coordinating proactive and reactive measures to shield these infrastructures. Additionally, cooperation with international organizations, alongside awareness-raising and training programs, significantly enhances the defense against threats to these critical systems. This article provides a comprehensive review of Critical Information Infrastructure Protection (CIIP) in Albania, emphasizing the pivotal role of the Cyber Incident Response Team (CSIRTs) and the necessity for robust protective measures aligned with both national and European cybersecurity regulations. It concludes with key recommendations for refining protective strategies and announces future studies aimed at analyzing historical trends and data to enhance the understanding and performance of CSIRTs among various stakeholders.

Key words**:** *critical information infrastructure, essential services, cybersecurity, international collaboration .*

Përmbledhje:

Që nga krijimi i internetit, mbrojtja e infrastrukturës kritike të informacionit ka qenë thelbësore, veçanërisht sepse sulmet ndaj këtyre sistemeve kanë një

ndikim gjithnjë e më të madh në të gjitha sektorët jetikë. Kjo mbrojtje është një përgjegjësi e përbashkët e ndarë midis sektorëve publik dhe privat. Në Shqipëri, Autoriteti Kombëtar për Sigurinë Kibernetike (NACS) vepron si Ekipi Kombëtar i Përgjigjes ndaj Emergjencave Kibernetike (CERT), duke koordinuar masat proaktive dhe reaktive për të mbrojtur këto infrastruktura. Gjithashtu, bashkëpunimi me organizata ndërkombëtare, së bashku me programet e ngritjes së ndërgjegjësimit dhe trajnimit, rrit në mënyrë të konsiderueshme mbrojtjen kundër kërcënimeve ndaj këtyre sistemeve kritike. Ky artikull ofron një përmbledhje të gjithanshme të Mbrojtjes së Infrastrukturës Kritike të Informacionit (CIIP) në Shqipëri, duke theksuar rolin vendimtar të Ekipit të Përgjigjes ndaj Incidenteve Kibernetike (CSIRTs) dhe nevojën për masa mbrojtëse të forta të përshtatura me rregulloret kombëtare dhe evropiane të sigurisë kibernetike. Artikulli përfundon me rekomandime kyçe për përmirësimin e strategjive mbrojtëse dhe rekomandon studime të ardhshme të synuara për të analizuar trendet historike dhe të dhënat për të përmirësuar ngritjen dhe funksionimin e CSIRT-ve ndërmjet palëve të ndryshme të interesit.

Fjalë kyçe: *infrastruktura kritike e informacionit, shërbimet kritike, siguria kibernetike, bashkëpunimi ndërkombëtar.*

Introduction

Communication networks and information systems have become an essential factor in economic and social development. As posited by various scholars, computing and networking are now considered as necessary services as electricity and water supply (Johnson, 2013). These systems not only support daily operations but also enable vital societal functions, underscoring their integral role in modern infrastructure. The security of communication networks and information systems, particularly their availability, is a growing concern due to the complexity of the systems, potential accidents, errors, and attacks against the physical infrastructures. These infrastructures provide critical services essential for the well-being of citizens (Smith et al. 2011). The increased reliance on these systems highlights their vulnerabilities and the profound impacts disruptions can have on societal functions. The rapid and complex development of technology has highlighted the need to define and protect critical infrastructures.

All countries require substantial support from their security structures to mitigate the risks associated with these new technologies (Christensen et al., 2017). Facing these risks involves a shared responsibility among international and national structures, extending to private industry, which often owns and operates these critical infrastructures, governmental bodies, and citizens themselves (Sontan et al., 2024). Hence, the creation and operation of a structure for the management of computer security incidents, known as Computer Incident Response Teams (CIRTs), is crucial. These entities not only respond to security breaches but also enable government and private sector stakeholders to better understand and react to cyber threats through robust incident management (Pashaj & Tomco, 2019). The risks associated with cyber- attacks are perpetually increasing, with threats from unknown sources continuously evolving. There is a significant emphasis in media reports on serious security incidents, illustrating a growing need for effective cyber security management (Almahmoud et al., 2023). As these threats evolve, the role of Computer Incident Response Teams (CSIRTs) becomes more critical. CSIRTs are pivotal in gathering information and coordinating responses to cyber security incidents, playing an essential role in national and international cyber security strategies (Kaur et al., 2023).

The primary aim of this research is to elucidate effective practices for protecting Critical Information Infrastructures (CIIs) and to assess how these practices are being implemented in Albania. This study seeks to benchmark Albania's efforts against global best practices in the field.

Our research objectives in this study are:

1. **Identify Best Practices and Strategies:** To delineate the leading practices and strategic approaches employed globally for the protection of Critical Information Infrastructures.

2. **Examine the Role of CSIRT Teams:** To underscore the critical role that Cyber Incident Response Teams (CSIRT) play in safeguarding Critical Information Infrastructures.

3. **Analyse Albania's Protective Measures:** To scrutinize the specific measures adopted in Albania for the protection of its Critical Information Infrastructures.

4. **Recommend Improvements:** To formulate conclusions that aim to enhance Albania's protective efforts within the existing framework for Critical Information Infrastructure protection.

This study employs a deductive approach, leveraging scholarly articles and best practices outlined by the European Union in the realm of cyber security. Our analysis extends to reviewing both Albanian and international legislative frameworks. It incorporates an extensive array of sources, including, but not limited to, cyber security legal acts, strategies, regulations, and methodologies. Given the focus on Critical Information Infrastructures, the research adopts a comparative approach to examine how these infrastructures are treated within Albanian legislation relative to other international examples. This comparative analysis ensures that findings are contextualized within the Albanian legislative and operational landscape.

The study is structured into three primary sections:

The first section introduces the concept of Critical Information Infrastructures and discusses their significance at both national and international levels. It also explores the necessity of developing protective policies. The second section delves deeper into the policy-making aspects necessary for safeguarding these infrastructures. The third section, is dedicated exclusively to the role of Cyber Incident Response Teams (CSIRTs) in the protection of Critical Information Infrastructures, highlighting them as a best practice example.

1. Understanding Critical Information Infrastructures

1.1 What are Critical Information Infrastructures?

Critical Information Infrastructures (CII) were initially defined around 2001 by Swiss professors and researchers as components such as telecommunications, computers/software, internet, satellites, and optical fibers.

This definition extends to the entirety of interconnected computers and networks facilitating the flow of critical information among them (The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers, n.d.). In 2003, the G8 expanded on this by offering a guide on the "Principles of Protection of Critical

Information Infrastructures," focusing more on best practices than defining the term explicitly.

Further clarity was provided by the European Commission in 2005 in the Green Paper for a European Program on Critical Infrastructure Protection (EPCIP), defining CIIs as "ICT systems critical to the infrastructure or essential for the functioning of critical infrastructures" (European Commission, 2005).

Following this, various states developed their definitions, reflecting their national priorities and concerns. For instance, the African Union describes CII as essential for public safety and economic stability ("African Union Convention on Cyber Security and Personal Data Protection African Union," 2014), whereas in the United Kingdom, it encompasses all IT systems supporting national infrastructure.

Despite these variations, the definition by the Organization for Economic Cooperation and Development (OECD) in 2008 has gained broad acceptance, describing CII as interconnected information systems whose disruption would significantly impact national well-being (OECD, 2008).

1.2 Identification of Critical Information Infrastructures

Operators across public, semi-public, and private sectors provide a range of services, the criticality of which depends on their use by clients. Table 1 lists the sectors considered critical.

CII sectors
Banking and Finance Services
Central Government/Government Services
Telecommunications/Information and Communication Technology Sector
Emergency and Rescue Services
Electric Power Supply Services

Healthcare Services
Transportation/Logistics/Supply
Water Supply Services
Food Services
Environmental Protection

Table 1: CII sectors

The OECD notes that CIIs typically include information components supporting critical infrastructures or essential government services, and those vital for the national economy (OECD, 2008). The criteria for identifying CIIs, as outlined by ENISA, include economic impact, political/governmental time impact, and industrial/environmental geographical distribution (ENISA, n.d.).

Factors	**Impact**
Economic	Financial impact
Political/Governmental	Time impact
Industrial/Environmental	Geographical distribution
Health	Public and individual well-being

Table 2: CII identification factors

Identification involves assessing the impacts of potential disruptions in these sectors, guided by national laws such as Albania's Law No. 25/2024 on "Cyber Security," which mandates updating the list of CIIs biennially (AKSK, 2024).

1.3 Identification of threats to Critical Information Infrastructures

The safeguarding of critical information infrastructure (CII) is paramount for maintaining the stability and security of essential national services. This was

vividly demonstrated by the Iranian cyberattacks on Albania in July 2022 (Microsoft, 2022).

These attacks severely disrupted Albania's governmental digital infrastructure, hindering public services and exposing significant vulnerabilities within the country's cyber defenses. The incident highlighted the urgent need for comprehensive cybersecurity measures to protect CII from such hostile actions. Ensuring the protection of CII is crucial for the uninterrupted operation of critical services, the preservation of national security, and the maintenance of public trust in digital platforms.

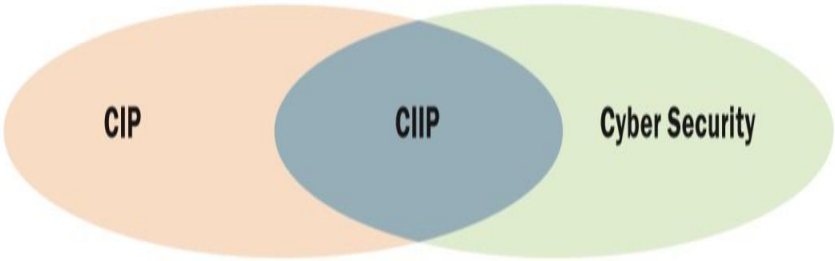
Albania's experience illustrates the potentially crippling effects of targeted cyberattacks on vital services, underscoring the necessity for vigilant surveillance, swift incident response, and thorough risk management. This event also brought to light the importance of international collaboration and support in countering cyber threats and bolstering the resilience of critical information infrastructure.

1.4 The need to protect Critical Information Infrastructures

The interconnected nature of modern infrastructures means that disruption in one area can lead to cascading effects across multiple sectors. CIIP is therefore crucial not only to protect national security but also to ensure the economic and social stability of a nation. This need is accentuated by the increasing reliance on ICT services, which are integral to the functioning of all critical infrastructures (European Commission, 2005).

Protection strategies must address both the physical and cyber aspects of CIIs to mitigate the broad spectrum of risks posed by modern threats.

Figure 1: The connection between CIP, CIIP, and Cybersecurity



In

Albania, the risks and threats to Critical Information Infrastructures is evaluated by the National Authority on Electronic Certification and Cyber Security. Official data of malware threats for 2023 have shown 151.186 IP vulnerable, which are affected by 60 malware families (AKSK, 2024).

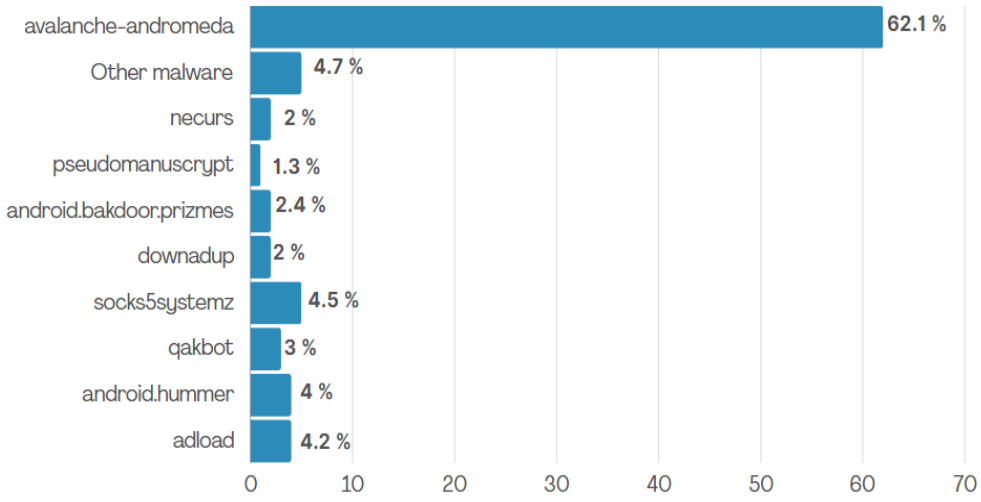


Figure 2 Threats, 2023. (Source: AKSK)

Moreover, in 2023 there were evaluated to be 23 559 vulnerable IP, as shown in below (AKSK, Vulnerable IP, 2024).

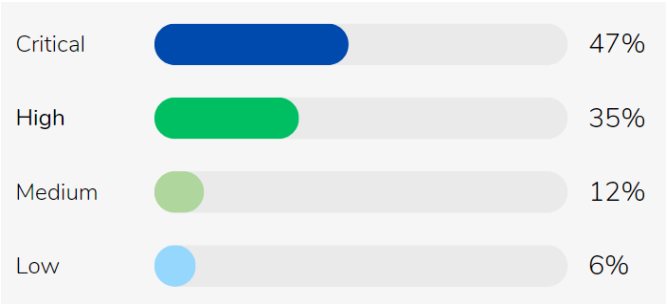


Figure 3 Vulnerable IP, 2023. (Source: AKSK)

2. Protection of Critical Information Infrastructure

The importance of Critical Information Infrastructure Protection (CIIP) has grown with the technological advancements and increasing cyber threats that have become prominent in the digital age. CIIP involves robust measures to safeguard systems and networks that are essential for the functioning of critical societal and economic activities. Effective CIIP strategies are vital to mitigate the risks of cyberattacks, which can disrupt public services, damage economies, and threaten national security.

Internationally, the implementation of CIIP strategies has varied significantly between countries, influenced by technological maturity, regulatory frameworks, and cybersecurity awareness. In Europe, the reception has been proactive, particularly with the European Union's directives aimed at strengthening cybersecurity measures across member states. The original NIS Directive laid the groundwork for national efforts, which has been recently updated to the NIS2 Directive, extending the security requirements to a wider range of sectors and emphasizing the importance of resilience against cyber threats (European Parliament, 2022). Similarly, the United States has integrated CIIP into its national security strategy, promoting a collaborative approach between the government and the private sector to protect critical infrastructures (U.S. Department of Homeland Security, 2018).

Albania's approach to CIIP has been met with a supportive but cautious attitude. The National Authority for Cyber Security (AKSK) leads the country's efforts, pushing forward initiatives to bolster cyber defenses. Despite this, Albania has encountered significant challenges, primarily due to limited human and technological resources. Early efforts were impeded by a scarcity of cybersecurity professionals and outdated technological infrastructure, which slowed the implementation of advanced CIIP measures (AKSK, 2020).

Statistical data from AKSK reveals improvements in Albania's cybersecurity posture. The 2023 report shows 49 cyber incidents reported to AKSK, 12 from which had an impact to the critical information infrastructure operators (AKSK official website, 2024). However, the annual report from the authority highlights ongoing issues with keeping technological tools up-to-date and providing continuous professional training in cybersecurity.

In response to these challenges, Albania has focused on upgrading its technological infrastructure and expanding educational programs in cybersecurity. The country has also sought to enhance its international collaborations to align with global best practices. However, financial constraints and the initial stage of technological adaptation have slowed the overall progress. Integrating CIIP strategies into Albania's broader national security framework remains an ongoing effort, with several strategic goals still to be fully realized (AKSK, 2020).

3. CSIRT as the Main Structure for the Protection of Critical Information Infrastructures in Albania

Per Law No. 2/2025 on Cyber Security, the National CSIRT of Albania holds a broad spectrum of responsibilities to ensure the security and seamless operation of critical information infrastructures. They are tasked with establishing secure communication channels for information exchange with operators and engaging with them through dedicated platforms for effective cyber incident management. The team diligently monitors, analyses, and manages national cyber threats, vulnerabilities, and incidents, providing technical support as needed.

Acting as the primary coordinator for identifying vulnerabilities in information networks, they collaborate with operators to address cyber incidents and work with law enforcement when cybercrime is suspected. The CSIRT issues warnings and disseminates information on potential risks and vulnerabilities, collects and analyses data through digital investigations, and retains logs of incidents for specified periods. They conduct proactive network scans to identify significant vulnerabilities and assess high-risk situations, taking reactive measures when necessary.

The CSIRT also verifies the implementation of cybersecurity measures, aids in resolving incidents, and formulates specific measures, communicating them to sectoral CSIRTs and operators. They develop guidelines, policies, and regulations to standardize incident management procedures, maintain an electronic registry of contact points, simulate networks to identify weak points, and analyse incident causes. International collaboration with CSIRT networks and coordination with law enforcement to preserve evidence in suspected cybercrime cases are also key aspects of their role.

The National CSIRT of Albania aligns with global CSIRT practices, emphasizing proactive communication, preventive measures, and extensive collaboration, tailored to the specific cybersecurity landscape of Albania.

According to the official data from AKSK (AKSK, Investments, 2024), the total budget in the field of cyber security for the year 2023 was 22,901,651 Euro of which 16,007,215 Euro were spent in this field.

For 2024, it is planned to increase the number of investments going to 28,272,119 Euro. This investment aims to improve protection in the digital space.

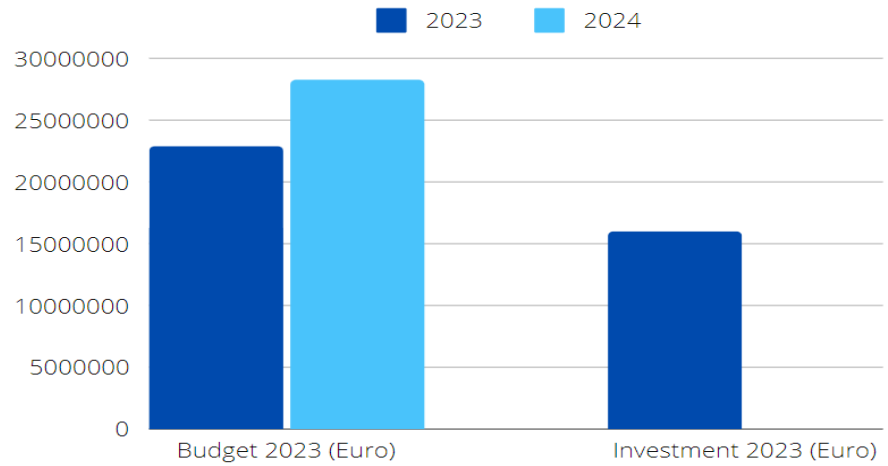


Figure 4 Investments, 2024. (Source: AKSK)

Technological Advancements and Policy Development

Albania aims to leverage cutting-edge technology to bolster its cybersecurity defences. This includes the adoption of advanced cybersecurity software and hardware, and the integration of artificial intelligence and machine learning technologies to enhance threat detection and response capabilities. Policy-wise, Albania is working on updating its national cybersecurity legislation and protocols to ensure they are in strict conformity with international standards such as those promulgated by the European Union's NIS2 Directive and

recommendations from the Council of Europe's Budapest Convention on Cybercrime.

Human Capital Development and International Cooperation

A crucial aspect of Albania's cybersecurity strategy involves human capital development. The Albanian government, in collaboration with academic institutions and international partners, plans to introduce specialized cybersecurity educational programs and training modules aimed at both new students and ongoing professional development for existing cybersecurity personnel. In terms of international cooperation, Albania has actively sought partnerships with various international bodies, including the European Union Agency for Cybersecurity (ENISA), the Organization for Security and Co-operation in Europe (OSCE), and the Geneva Centre for Security Sector Governance (DCAF). These collaborations are intended to facilitate knowledge exchange, foster best practices, and provide technical assistance in strengthening Albania's cybersecurity infrastructure.

The proactive development of CSIRTs capabilities offers numerous advantages to Albania, enhancing national security, protecting critical infrastructure, and ensuring the continuity of economic and governmental activities. Moreover, aligning with international cybersecurity standards helps improve Albania's standing on the global stage, potentially attracting more foreign investment and boosting economic growth. However, challenges such as limited financial resources, existing technological gaps, and the need for a larger skilled workforce remain significant obstacles. Additionally, as cyber threats evolve, there is an ongoing requirement to continuously update and adapt cybersecurity strategies and tools to stay ahead of potential attackers.

Conclusions and recommendations

This study has extensively explored the current landscape of Critical Information Infrastructure Protection (CIIP) in Albania, focusing on the integral role played by the Cyber Incident Response Team (CSIRT). Over the course of this research, it has become evident that while Albania has made significant strides in establishing and strengthening its cybersecurity measures, considerable challenges still lie ahead. The development of sectorial CSIRTs within Albania is crucial for safeguarding national security, economic stability, and the overall well-being of its citizens.

The analysis highlights the concerted efforts to align national practices with international standards, a move that has started yielding positive outcomes in enhancing Albania's cybersecurity posture. Through strategic advancements in technology adoption, policy formulation, and human capital development, Albania has begun to solidify its defensive capabilities against an increasingly complex array of cyber threats. Despite these advancements, several limitations remain evident in Albania's approach to CIIP. One of the primary constraints is the resource limitation, both in terms of financial investment and technical expertise. The cybersecurity landscape requires constant technological upgrades and a steady influx of skilled professionals, areas where Albania currently faces deficits.

Additionally, the pace of legislative and regulatory adaptations to the evolving cyber environment has been slower than needed. This delay in policy modernization poses a risk to maintaining a resilient cybersecurity posture, as threats evolve far more rapidly than the legal frameworks designed to combat them.

Looking forward, Albania faces both challenges and opportunities in its pursuit of enhanced CIIP. The next steps involve several key areas of development:

i. **Enhanced International Cooperation**: As cyber threats do not respect national boundaries, increasing international cooperation is paramount. Albania should seek to strengthen its ties with global cybersecurity organizations and neighbouring countries to enhance its threat intelligence and response capabilities.
ii. **Investment in Advanced Technologies**: The adoption of advanced technologies, such as artificial intelligence (AI) and machine learning, can provide Albania with the tools needed to anticipate, detect, and respond to cyber incidents more effectively. Investing in these technologies will also help bridge the current gap between Albania and more technologically advanced nations.
iii. **Expansion of Educational Programs**: Developing a robust educational framework that focuses on cybersecurity at all levels of education will be essential. This includes not only tertiary education but also continuous professional development courses and public awareness campaigns to cultivate a cybersecurity-conscious culture.

iv. **Policy and Legislative Reforms**: There is a pressing need for Albania to expedite its legislative reforms related to cybersecurity. This involves not only updating existing laws but also ensuring that these legal frameworks are adaptable to the fast-paced changes in the cyber domain.

v. **Building a Resilient Cybersecurity Culture**: Beyond technology and regulations, there is a critical need to establish a resilient cybersecurity culture across all sectors of society. This involves regular training, simulations, and drills to prepare for and effectively respond to cyber incidents.

vi. **Focus on Cybersecurity Research and Development (R&D)**: Establishing dedicated R&D centres for cybersecurity can significantly enhance Albania's capabilities. These centres would focus on developing new technologies and methodologies for cybersecurity, tailored to meet the unique challenges faced by the country.

vii. **Public-Private Partnerships**: Strengthening collaborations between the government and the private sector can lead to better resource allocation and more innovative solutions. These partnerships are crucial for sharing knowledge, technologies, and best practices in cybersecurity.

In conclusion, while Albania has established a solid foundation for the protection of its critical information infrastructures, the journey is far from complete. The forthcoming years will be critical in determining how well Albania can adapt to the global cybersecurity landscape. With strategic investments in technology, human resources, and international partnerships, Albania can aspire to not only meet but exceed the current standards, ensuring a secure and resilient digital future. Additionally, the availability of more comprehensive and diverse data opens the door to dynamic analysis and model development. These next steps will help institutions, agencies and more to better understand their cybersecurity posture and take more effective measures to reduce potential risks.

References

African Union Convention on Cyber Security and Personal Data Protection | African Union. (2014). Retrieved from au.int website: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

AKSK. (2018). Metodologjia e punes CSIRT. Retrieved from AKSK website:

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

AKSK (2020) Strategjia Kombëtare për Sigurinë Kibernetike

strategjia_kombetare_sigurise_kibernetike-2.pdf (cesk.gov.al)

AKSK. (2023). Metodologji për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit. Retrieved from

https://cesk.gov.al/wp-content/uploads/2023/09/Metodologjia.pdf

AKSK (2024) Ligji Nr. 25/2024 "Për Sigurinë Kibernetike" Për sigurinë kibernetike (cesk.gov.al)

AKSK. (2024). *Vulnerable IP*. LinkedIn.

https://www.linkedin.com/feed/update/urn:li:activity:7185583321622470658 AKSK. (2024). *Threats*. LinkedIn.

https://www.linkedin.com/feed/update/urn:li:activity:7185665659823923202

AKSK (2024) Investments, LinkedIn

https://www.linkedin.com/feed/update/urn:li:activity:7183111289936695296

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Retrieved April 28, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

Christensen K.K., Petersen K.L. (2017) Public–private partnerships on cyber security: a practice of loyalty, International Affairs, Volume 93, Issue 6, November 2017, Pages 1435–1452, https://doi.org/10.1093/ia/iix189

Johnson, C. W. (2013). The Telecoms Inclusion Principle. *IGI Global EBooks*, 277–303. https://doi.org/10.4018/978-1-4666-2964-6.ch014

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*, *97*(101804), 101804. https://doi.org/10.1016/j.inffus.2023.101804

Pashaj, K. Tomco, V. (2019, May 21). Policimi dhe siguria nr. 12 [proceedings] by Policimi dhe siguria - Issuu.

https://issuu.com/policimi.dhe.siguria/docs/policimi_dhe_siguria_12_proceedings

Sontan Adewale Daniel, & Samuel Segun Victor. (2024). Emerging trends in cybersecurity for critical infrastructure protection: a comprehensive review. Computer science & it research journal, 5(3), 576-593. https://doi.org/10.51594/csitrj.v5i3.872

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

ENISA. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. Retrieved April 28, 2024,

https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

European Commission. (2005). Green Paper on a European Programme for Critical Infrastructure Protection. Retrieved from

https://eurex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=BG

G8. (2003). G8 Principles for Protecting Critical Information Infrastructures.

http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

Microsoft (2022, September 8). Microsoft investigates Iranian attacks against the Albanian government. Microsoft Security Blog. https://www.microsoft.com/en-

us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Oecd. (n.d.). 2 -oecd recommendation of the council on the protection of critical information infrastructures organisation for economic Co-Operation And Development. Retrieved from http://www.oecd.org/sti/40825404.pdf

PayPal Breach Exposed PII of Nearly 35K Accounts. (n.d.). www.darkreading.com. https://www.darkreading.com/cyberattacks-data-breaches/paypal-breach-exposed-pii-of-nearly-35k-accounts

Smith, H.J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Q., 35, 989-1015. https://doi.org/10.2307/41409970

Sontan Adewale Daniel, & Samuel Segun Victor. (2024). Emerging trends in cybersecurity for critical infrastructure protection: a comprehensive review. Computer Science & IT Research Journal, 5(3), 576-593. https://doi.org/10.51594/csitrj.v5i3.872

The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. (n.d.).

https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

U.S. Department of Homeland Security. (2018). National Cyber Security Strategy. Retrieved from https://www.dhs.gov/publication/national-cyber-strategy-2018

Zaid Almahmoud, Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. *Nature.com*, *13*(1).

https://doi.org/10.1038/s41598-023-35198-1