CHALLENGING THE ALBANIAN E.U. CYBERSECURITY PERSPECTIVES

Reis Mulita

Center for Innovation, Research and Development, Faculty of Economy, Canadian Institute of Technology, reis.mulita@cit.edu.al, ORCID: 0000-0003-3911-469X

Abstract:
Cybersecurity has emerged as a critical concern on a global scale, and Albania is no exception. This paper delves into Albania's current cybersecurity challenges, shedding light on existing vulnerabilities and presenting recommendations to enhance the nation's resilience against cyber threats, considering the country's E.U. perspectives. The paper explores critical facets of cybersecurity, including the vulnerabilities within the country's infrastructure, the regulatory framework, and the prevalent skills gap. By addressing these aspects, a comprehensive overview is provided, outlining Albania's challenges in safeguarding its digital assets.

The methodology used in this paper applies a theoretical approach based mainly on qualitative methods using secondary data and information, analyzing, comparing, and evaluating sources coming mainly from secondary sources, national and international ones. Through this method, the paper aims to offer a nuanced understanding of the cybersecurity landscape in Albania and its E.U. challenges regarding cybersecurity perspectives.

In summary, this research concludes that by addressing cybersecurity challenges, Albania will be more effectively integrated into the E.U. and the global market economy, benefiting well-being and creating a more secure society.

Keywords: Cybersecurity, Albania, E.U. Challenges, Cybersecurity Index, Regulations;

Introduction

It is well-known that the global economy heavily relies on the widespread adoption of Information Communication Technology (ICT) and internet connectivity. The digital agenda of every E.U. country promises to enhance service delivery, promote good governance, improve efficiency, drive innovation and productivity gains, and boost economic growth (European Commission,2015). However, the availability, integrity, and resilience of this critical infrastructure are under threat (Giaccone, A. 2019). The sophistication of threats to networked systems and infrastructures is increasing. Data breaches, criminal activities, property destruction, and service disruptions pose significant risks to the Internet economy. Albania also suffered continuing cyberattacks, digitally devastating the country's critical computerized public and private infrastructure starting in 2021(Oghanna, A.,2023). Cybersecurity is crucial for digital trust in various structures (Mulligan, C. 2017). It Is considered the cornerstone of the digital economy and determines the level of Trust that digital information users have in various economic and social structures and government regulations. Shein at Tech Republic (2022) shows that Sixty-five percent of defenders report an increase in cyberattacks since Russia's invasion of Ukraine, according to VMware's eighth annual Global Incident Response Threat Report, released at Black Hat USA 2022. The World Economic Forum has identified cybersecurity as one of the most severe risks to further development. Estimates suggest cyberattack losses could reach $3 to $6 trillion by 2021(World Economic Forum, 2019). The increasing reliance on digital technologies in Albania has brought about unprecedented economic growth and societal advancement opportunities. However, this digital transformation has also exposed the nation to many cybersecurity challenges. To face these challenges successfully, cybersecurity is currently a top priority for the Government AKCESK (2023). Albania is one of the most advanced countries in the Western Balkans region regarding cybersecurity regulations (AKCESK, 2022).

Evidence has shown that countries must ensure that their economic objectives align with their security priorities to achieve overall national development and security (World Economic Forum, 2019). Also, there will be a close connection between human and machine intelligence in the future, and the quality of this interaction will depend on various factors, including the level of human resource development(Frontier Economics,

*Corresponding author:

2011). Currently, organizations are facing a shortage of highly skilled professionals (Hays et al., 2017). They are trying to overcome this by implementing corporate systems for personnel development and talent management and collaborating with higher education institutions. Any disparity between these can lead to significant issues and challenges, so Albania must align its national economic vision with national security priorities for a stable and prosperous future. Considering the mentioned assumptions, this paper aims to explore and analyze Albania's specific cybersecurity challenges, highlighting the need for proactive measures to secure its digital landscape.

The E.U. Cyber Security Challenges and Perspectives

The term 'digital sovereignty' may have different meanings in different contexts, ranging from 'nation-state sovereignty' to 'personal technological sovereignty (Couture et al.; S., 2018). These contexts extend from individual citizens to social movements and include entire countries. European digital sovereignty has three aspects: people, industry, and politics (EU JOIN, 2017). Strategic autonomy refers to the capacity and capabilities to decide and act on essential aspects of a society's longer-term future in the economy and institutions. Timmers, P. (2019). Digital strategic autonomy can be defined as Europe's capability to acquire products and services that meet its requirements and principles without being subjected to any undue influence from external sources. The needs of consumers may require various products and services, including hardware, software, or algorithms. The European Union Agency for Cybersecurity has identified critical topics in cybersecurity research and innovation to achieve specific strategic objectives. In 2018, the primary aim was to enhance cybersecurity in the E.U. (ENISA, 2018). This document, which is the second in the series, is intended to support the E.U.'s digital strategic autonomy. Artificial Intelligence (AI) is becoming increasingly important for daily and critical services, such as energy production and distribution, transportation management, and healthcare infrastructure. Trusting the data and algorithms that process it is essential for a secure and reliable digital society. The issue in question is the risk of losing control over information and the algorithms processing it. However, the E.U. has taken the initiative to protect E.U. citizens. (ENISA, 2018). Artificial Intelligence (A.I.) plays a crucial role in driving several daily and critical services, such as energy production and distribution, transportation management, and healthcare infrastructure. However, to ensure that our digital society is trustworthy, we must be able to rely on the data and algorithms that process it. The primary concern is the risk of losing control over the information and the algorithms processing it. The European Union (E.U.) has taken the lead in protecting E.U. citizens, but more work needs to be done to secure our data (ENISA, 2018:11). Data protection is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights (EU COM, 2012). The introduction of the General Data Protection Regulation (GDPR) has created an obligation to protect E.U. personal data. The GDPR has had a worldwide impact on countries and businesses, leading to changes in laws and practices outside of Europe as well.

The digitalization of society has introduced digital controls in many new places, which has created more opportunities for attackers to gain easy access. Unfortunately, product designers focus more on functionality and less on security, making it easier for attackers to exploit vulnerabilities. For example, from 2017 to 2018, 80% of the vulnerabilities found in medical devices were exploiting network access, and 40% could be triggered remotely with basic skills and no particular privileges (Debar, H.2019). Ensuring digital autonomy and sovereignty requires technological leadership and a solid legal and regulatory framework for research and development. The E.U. must guarantee access to a competent workforce to design, operate, and audit critical infrastructure services. Europe is facing a shortage of cybersecurity experts, which makes it challenging to retain these skilled professionals. To tackle this problem, Europe needs to develop its own cybersecurity skills framework. This framework will help create a common language for individuals, employers, and training providers, making it easier to identify the required skills. By doing so, businesses and governments can have access to a sufficient number of skilled professionals, which will help Europe maintain its leadership in the field of cybersecurity (ENISA, 2023).

Methodology

This paper will address answers to the main research question: What are Albania's critical cyber security challenges and vulnerabilities in the current digital landscape, and how can the country enhance its cyber resilience to mitigate and respond effectively to emerging cyber threats of the E.U. 2030 foresight? One methodology used to reduce the cost of cyberattacks is CRI 2.0. It provides a framework for countries to pursue economic growth securely while maintaining resilience. The Cyber Readiness Index (CRI) 2.0 has two main components (Potomac Institute for Policy Studies, 2015). Firstly, it provides national leaders with objective evaluations of their countries' maturity and commitment to cybersecurity and resilience. This information is essential for leaders to protect their increasingly connected countries with a potential for GDP growth. Additionally, the Cyber Readiness Index (CRI) explains what it means for a country to be "cyber-ready" and provides a blueprint to achieve this status. This methodology provides a valuable and straightforward tool to assess the gap between a nation's cybersecurity posture and national cyber capabilities to achieve its economic vision. The blueprint used for this analysis includes over seventy unique data indicators across seven elements. There are seven key elements to a national cybersecurity framework: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development (R&D), diplomacy and trade, and defense and crisis response.

The assessment of each country's cyber readiness is based on primary sources, grounded on empirical research and documentation. Countries are evaluated based on three levels of cyber readiness: insufficient evidence, partially operational, or fully operational. The CRI 2.0 methodology evaluates 125 countries' cyber readiness based on their maturity and commitment to cybersecurity, resilient infrastructures, and services. More information about CRI 2.0 is in Figures 1 and 2(Potomac Policy Institute, 2015). Albania is not included in these assessments due to the methodology used in the CRI 2.0. The selection of countries includes the top 75 countries from the International Telecommunication Union (ITU, 2023) ICT Development Index (IDI), highlighting the importance of connectivity. Albania was not included in this assessment. Nevertheless, as we can see, facing the challenges of cyber-attacks, no country was ready, as a conclusion came from the CRI 2.0 Report 2-15. This report was chosen as an initial reference part for the measurements. The CRI 2.0 methodology consists of seven essential elements. Each element has at least ten supporting indicators for evaluation. These indicators provide a blueprint of a country's cyber readiness when combined. Below, you will find a detailed description of each essential element and its supporting indicators. Additionally, the text includes country examples that showcase innovative and multicultural solutions for achieving cyber-readiness. Although these examples are not exhaustive, they demonstrate unique country-level approaches. Having a clear and published National Cyber Security Strategy that aligns with the country's economic vision and security requirements is a crucial indicator of a country's readiness in the cyber domain. A country's digital economy and future depend on the Internet, broadband networks, mobile applications, I.T. services, software, and hardware, which form the foundation of the digital infrastructure (OECD,2015). A National Cybersecurity Strategy outlines how to allocate resources to prioritize national cybersecurity objectives, improving a country's security and resilience. The Strategy should identify the national cybersecurity objectives and the governance structure for their implementation (U.N., 2021). It is important for a country to have a strong incident response capability in place in order to show its readiness to tackle cyber threats. Such capability is often managed by one or more teams, such as the National Computer Security Incident Response Teams (National CSIRTs) or Computer Emergency Response Teams (Naseir, 2023). These teams, collectively known as CSIRTs, manage incident response in natural or manufactured cyber-related disasters that affect critical services and information infrastructures. (ITU, 2023).

Ensuring a country's cyber readiness involves three essential elements. One of the critical elements is the country's commitment to safeguard its society against cybercrime. As cybercrime is a global problem that transcends national borders, it requires international solutions. Therefore, countries must demonstrate their commitment to secure their society against e-crime by taking collective international actions. One way of measuring a country's readiness to tackle cybercrime is by assessing its commitment to implementing transnational solutions. Legislation plays a vital role in creating a framework for organizations to comply with regulatory standards. It can include rules against particular criminal behavior or establish minimum regulatory requirements. Setting up and maintaining information-sharing mechanisms is a critical factor in determining a nation's readiness for cyber threats. These mechanisms help exchange intelligence and information between different sectors of the Government and industries, which can help identify, assess, and respond to targeted activities. Sharing threat and intelligence information can help us understand how different sectors are targeted, how information is lost, and how we can defend our information assets better. There are four models for information sharing that have emerged to address cyber threats and secure information assets. Capacity development is an essential component of legal, technical, and organizational measures within the Global Cybersecurity Index and is a driving force for digital development. Capacity development programs aim to build local skills, knowledge, and confidence, which can help close the skills gap and build a more inclusive technology ecosystem. Moreover, delivering inclusive digital services increasingly relies on a skilled workforce. Capacity development frameworks for promoting cybersecurity may include awareness-raising, research and development programs, education and training programs, and certified professionals and public sector agencies. These frameworks can be used to measure their effectiveness. (Hays et al., 2017). Another vital element that indicates a country's readiness to deal with cyber threats is establishing a national priority for and investment in cyber security basic and applied research, as well as ICT initiatives broadly. The advancement of ICT has transformed almost every sector of the economy, revolutionizing businesses, governments, education, and how citizens live, work, and play.

These innovations drive economic growth and can enhance resilience, laying the foundation for solid security measures. Cybersecurity spans sectors, geographic, and resource levels, so cooperation is needed at the private, public, regional, and international levels. More outstanding cooperative initiatives can develop much more robust cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension, and prosecution of malicious agents. (ITU GCIv5, 2022).

The Global Cybersecurity Index Indicators

The Global Cybersecurity Index (GCI) is a benchmark that measures and compares countries' commitment to cybersecurity across the five pillars of the Global Cybersecurity Agenda (GCA). The ITU framework aims to build synergies between current and future initiatives and focuses on five pillars: legal, technical, capacity building, organizational, and cooperation. To calculate the GCI, a questionnaire with 82 binary, pre-coded, and open-ended questions was used (ENISA, 2023). This provided a value for 20 indicators, selected based on relevance to the five GCA pillars, the main GCI objectives and conceptual framework, data availability and quality, and the possibility of cross-verification through secondary data (Hathaway, M.2015).

The Foresight Exercise Methodology Overview was implemented through a series of workshops and interviews between March and August 2022. Experts in the PESTLE fields (political, economic, social, technological, legal, and environmental) were consulted during these sessions. The methodology used comprises of four phases. The first phase is called "collaborative exploration," which involves researching and gathering information on current trends while integrating expert knowledge, feedback, and validation. The second phase, called "group forecast workshops," involves bringing together groups of experts with experience in one of the PESTLE dimensions. They discuss, explore, assess, and prioritize the identified trends. The third phase, "threat identification," employs the threat casting methodology to identify emerging challenges that will increase in prevalence by 2030. ENISA has identified and ranked 21 such threats. The strategic objectives of this exercise are to empower and engage communities within the cybersecurity ecosystem, make cybersecurity an integral part of E.U. policies, establish practical cooperation among operational actors within the Union in case of massive cyber incidents, develop cutting-edge competencies and capabilities in cybersecurity across the Union, promote a high level of trust in secure digital solutions, have foresight on emerging and future cybersecurity challenges and to ensure efficient and effective cybersecurity information and knowledge management for all.

As an agency of the European Union, the European Union Agency for Cybersecurity (ENISA) is devoted to promoting a high level of cybersecurity across Europe. ENISA, with the support of experts, identified and ranked the top 10 cybersecurity threats that may emerge by 2030 during an 8-month foresight exercise. They conducted a Threat Identification Workshop to brainstorm solutions for the upcoming challenges in 2030.

In Albania throughout 2022, AKCESK (National Authority for Electronic Certification and Cyber Security) has been working on updating the current legal basis, including Law No. 9880/2008, "On the electronic signature," Law No. 107/2015, "On electronic identification and trusted services," and Law no. 2/2017 "On cyber security ."These updates are being implemented in full compliance with the European Regulation IDAS No. 910/2014, which deals with electronic identification and trusted services for electronic transactions within the E.U. Additionally, they adhere to the European Parliament and the Council have implemented Directive (E.U.) 2016/1148, also known as the NIS Directive, to ensure a uniform level of security for networks and information systems across the European Union. Any spelling, grammar, or punctuation errors have been corrected. The proposed legislation titled "Electronic Identification and Trusted Services Act" aims to establish a framework for reliable electronic identification and digital trust services in the country. The draft law outlines the legal and technical requirements for the use of electronic identification, such as digital signatures, seals, and time stamps, and establishes the responsibilities of the relevant authorities and service providers. This legislation is crucial for promoting the use of electronic transactions and increasing confidence in the security and integrity of digital services. The accompanying package was issued for public consultation on 07.12.2022, and the process ended on 10.01.2023. The bill is currently being revised based on the feedback provided by institutions and interested parties. The goal is to submit the revised draft law within the first three months of 2023. As for the "Cyber Security" draft law, the final version has been developed. However, with the adoption of the NIS2 Directive in December 2022, the draft law was revised to include some elements of this Directive. The complete package was also prepared for further public consultation.

Discussion

Albania is one of the 193-member states of the U.N. specialized agency that works together to advance the development of information and communication technology worldwide, upholding a long-established tradition of consensus. A national cybersecurity strategy (NCS) is a vital component of organizational measures at the national level. According to the ITU Guide to Developing a National Cybersecurity Strategy (ITU, 2023), an NCS is a comprehensive framework or Strategy that must be developed, implemented, and executed through a multi-stakeholder approach. It aims to facilitate coordinated action for preventing cyber threats, preparing for potential risks, responding to incidents, and recovering from any damages caused. This approach involves government authorities, the private sector, and civil society working together to ensure the safety and security of national cyberspace.

Albania first established the National Cyber Defense Strategy in 2014(Gov Al,2014). Through this Strategy, the Albanian Government has established 6(six) main priorities and focus activities following the CRI 2.0 strategy. According to the Strategy in matter the following objectives will be achieved through the following strategic pillars: Implementing a comprehensive and systematic approach to ensure the security of systems and information, enhancing the cyber defense of M/M and F.A. by improving the communication and information systems infrastructure, cultivating a culture of change, awareness, and innovation in the Ministry of Defense for Cyberspace to enhance knowledge and skills of users and specialists in detecting, addressing, alerting, and responding to incidents occurring in the systems and information, developing the skills of users and specialists to discover, address, alert and respond to incidents occurring in the systems and information, strengthening the intelligence position in cyberspace, strengthening cooperation at the national and international level, and partnering with businesses to ensure the security and sustainability of infrastructure, computer networks, and the products and services they provide(Gov Al,14: 4-5). The Government of Albania has also approved the new National Cybersecurity Strategy for the period of 2020 to 2025(Geneva et al., 2023). This comprehensive document provides a clear roadmap for the country to improve its cybersecurity landscape. The Strategy was developed in line with the 'National Security Strategy 2014-2020' and the Cybersecurity Policy Paper 2014-2017.

ITU has, to date, completed CIRT assessments for more than 80 countries. Albania is one of these countries listed (ITU, 2023). Based on the Country's Comparison of the indicators found in the ITU statistics (ITU, Datahub.itu.int/indicators, 2023), this paper analyses the following arguments

a. Households with internet access at home.

Based on the comparison of the countries above, the reasons for the highest usage of home Internet in Albania might be:

- Phone deals that include Giga bite internet cost a lot of money and offer minimal giga bite internet for use, while the home deals for the Internet are more economical;
- Lower monthly payments of employees compared to the salaries of other countries and lower general incomes for the population;
- Increase in the population's interest in surfing the Internet and using social networks such as Instagram, Facebook, Tiktok, YouTube, etc;

b. Investment in telecommunication services;

Based on the comparison of the countries above, Greece has the highest investments in telecommunication services, and the second country in the Balkans, with the highest investments after Greece, is Serbia, with a difference of $261M lower than Greece.

Greece is a European country, which makes it have more income and financing for investments in their country, but it also has complied with the European and international obligations and standards to invest in telecommunication services and infrastructures;

- Albania, North Macedonia, and Montenegro have a deficient percentage of investments in telecommunication services compared to Serbia and Greece since they also have a lower income compared to both the other countries;
- Financing or donations from third parties for investment in the technology and telecommunication field would be significant for countries such as Albania, Macedonia, and Montenegro;

c. ICT regulators that have in place for Cybersecurity mandate

- In Albania, it covers the area of Critical information infrastructure protection, and actually, we have it based on the Decision of the Council of Ministers No. 553, dated 15.07.2020, "On the approval of the list of critical information infrastructures and the list of important information infrastructures," and AKCESK is the State Authority that is responsible for its implementation and audit.
- North Macedonia covers the area of Network security, while Serbia has not specified the area covered by this framework that it has in place.
- It is important to note that Montenegro and Greece have yet to implement a cybersecurity framework and mandate. Due to the fact that technology is rapidly evolving each day, the potential level of risk is also increasing. This makes these two countries more vulnerable in the cyber environment.
- Albania experienced a cyber-attacks situation starting in 2021. Foreign Policy Magazine (Oghanna, A. 2023) reports that Albania has been experiencing a series of cyberattacks wreaking havoc on its critical computerized public and private infrastructure.

The hackers gained continuous access to Albanian government servers in 2021, which caused them to harvest data before launching a destructive "wiper" attack. This involved using ransomware and disk-wiping malware to destroy public data in July 2022.

Conclusion

This paper emphasizes the urgent need to address cybersecurity challenges in Albania and how comprehensive legal reforms, technological advancements, and capacity building can enhance the country's cybersecurity, challenging its E.U. perspectives.

Through different evidence, it is concluded that even E.U. countries are not fully prepared for cyberattacks. Challenging the Albanian E.U. perspectives, the national cybersecurity actions must reflect cybersecurity's socio-economic and environmental importance.

The resilience of critical services is crucial for national security and economic development in Albania. Cybercrime and fraud hinder economic growth, making it crucial to reduce the number of infected networked devices to combat e-crime.

Trust and buy-in from all stakeholders are necessary to facilitate information sharing. Real-time actionable information plays a critical role in mitigating cyber threats, while cybersecurity R&D innovation should focus on enhancing Trust, security, and resilience in our future networked society.

Collaboration among different parties in the realm of cybersecurity aims to achieve solutions that are mutually acceptable and address shared challenges. Cybersecurity is intertwined with every aspect of trade and foreign policy, making it a crucial area of focus. In order to effectively defend against cyberattacks that cause disruptions and destruction, a credible cyber defense is essential.

Albania must align with ENISA's Strategy proposed with seven strategic objectives that will set the priorities for the European Union Agency for Cybersecurity in the coming years. Dependence on electronic communications, bio revolution, and combinational weapons make reducing cyber threats imperative.

References

1. AKCESK, (2023). A safe cyber ecosystem for Albania. Cybersecurity Strategic visions. https://cesk.gov.al/en/a-safe-cyber-ecosystem-for-albania;

2. AKCESK, (2022). Raporti Vjetor 2022. https://cesk.gov.al/en/category/annual-reports;

3. COM, (2012). European Union, Charter of Fundamental Rights of the European Union, C 326/02, Brussels, 26.10.2012, pp. 391–407;

4. Couture, S. and Toupin, S. (2018). 'What does the concept of "sovereignty" mean in digital, network and technological sovereignty?', paper presented at Giga Net: Global Internet Governance Academic Network, Annual Symposium 2017, 2018 (http://dx.doi.org/10.2139/ssrn.3107272);

5. Debar, H., (2019). Vulnerabilities in the Internet of Medical Things, FOSAD;

6. ENISA. (2021), Analysis of European R&D Priorities in Cybersecurity. https://www.enisa.europa.eu/topic;

7. ENISA. (2020, March). Raising Awareness of Cyber Security. https://www.enisa.europa.eu/topics

8. ENISA. (2021). Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity

9. ENISA. (2019). Blockchain. Retrieved from https://www.enisa.europa.eu/topics/csirts-ineurope/glossary/blockchain;

10. ENISA. (2023). Identifying Emerging Cyber Threats and Challenges for 2030. https://www.enisa.europa.eu/publications/foresight-challenges;

11. E.U. Join (2017). European Commission, Joint Communication to the European Parliament and the Council – Resilience, deterrence, and defense: Building strong cybersecurity for the E.U., JOIN(2017) 250 final, Brussels, 13.9.2017.

12. European Commission, "Digital Single Market: Bringing down the barriers to unlock online opportunities," http://ec.europa.eu/priorities/digital-single-market;

13. European Union, Regulation (E.U.) (2016). /679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/E.C. (General et al. L 119), Brussels, 4.5.2016, p. 1–88 (https://eur-lex.europa.eu/eli/reg/2016/679/oj);

14. Frontier Economics (2011). Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy, London;

15. Geneva Digital Watch, (2020).

16. Giaccone, A. (2019). Under Attack: Trading Digitally in the Age of Vulnerability. https://core.ac.uk/download/214176549.pdf;

17. Gov Al, (2021). Albanian National Strategy on Cyber Defense. Republic of Albania. Ministry of Defense. https://cesk.gov.al/wp-content/uploads/2023/06/National-Cybersecurity-Strategy-and-its-Action-Plan-2020-2025.pdf;

18. Hays Global Skills Index (2017). Regional dynamics of the global market: skills in demand and tomorrow's workforce. 56 p;

19. ITU, (2023). Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E;

20. ITU, (2023). National Computer Security Incident Response Teams (National CSIRTs). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx;

21. ITU GClv5(2022). www.itu.int/en/ITUD/Cybersecurity/Pages/global-cybersecurity-index.aspx

22. Hathaway, M. (2015). Cyber Readiness Index 2.0 A PLAN FOR CYBER READINESS: A BASELINE AND AN INDEX. Potomac Institute for Policy Studies. Arlington, USA;

23. Mulligan, C. 2017, Cybersecurity: the cornerstone of the digital economy, available at: https://www.imperial.ac.uk/business-school/knowledge/technology/cybersecurity-cornerstone-of-the-digital economy;

24. Naseir, M. A. B. (2020). National cybersecurity capacity building framework for countries in a transitional phase. University of Bournemouth. U.K. https://core.ac.uk/download/430162063.pdf

25. Potomac Institute for Policy Studies, (2015). Cyber Readiness Index 2.0 A plan for cyber readiness: a baseline and an index. Arlington, USA;

26. OECD, (2015). OECD Digital Economy Outlook. Paris, France: OECD Publishing), http://dx.doi. of national Cyber Security Strategies, org/10.1787/9789264232440-en;

27. Oghanna, A. (2023). How Albania Became a Target for Cyberattacks. Foreign Policy Magazine. USA. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran. WDC. The USA.

28. Peter C. Evans and Marco Annunziata (2012), "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric. https://www.techrepublic.com/article/deepfake-attacks-and-cyberextortion-are-creating-mounting-risks/;

29. Shein, E. (2022). Deepfake attacks and cyber extortion are creating mounting risks. Tech Republic.https://www.techrepublic.com/article/deepfake-attacks-and-cyber-extortion-are-creating-mounting-risks;

30. Timmers, P. (2019). Ethics of A.I. and Cybersecurity When Sovereignty is at Stake. Minds and Machines. Springer.https://doi.org/10.1007/s11023-019-09508-4;

31. International Telecommunications Union, (2019). "CIRT Programme," http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx;

32. World Bank, "Overview," Information & Communication Technologies Program, last modified 2 October 2014, http://worldbank.org/en/topic/ict/overview;

33. World Economic Forum, (2019). Global Risk Report 2019, 14th Edition, p.114.

34. ITU, Datahub. Itu. int/indicators;

35. UN NCS, (2021). NCS Guide 2021. https://ncsguide.org/the-guide;