CYBER (IN)SECURITY IN BOSNIA AND HERZEGOVINA: CHALLENGES AND PERSPECTIVES

Jasmin Ahić[1]
University of Sarajevo, Faculty of Criminal Justice and Security Studies

Nerma Halilović-Kibrić[2]
University of Sarajevo, Faculty of Criminal Justice and Security Studies

Abstract: This paper examines the current state of cyber security in Bosnia and Herzegovina, focusing on legislative frameworks, incidents of cyber attacks, and potential avenues for advancement in line with Bosnia and Herzegovina's aspirations for European Union membership. This analysis highlights the urgent need for comprehensive cyber security legislation that aligns with the EU's Network and Information Security (NIS) Directive. Bosnia and Herzegovina has experienced numerous cyber attacks, including ransomware incidents, phishing campaigns, and DDoS attacks. These incidents underscore significant deficiencies in protecting critical infrastructure and IT systems. Case studies reveal that government institutions, the financial sector, and educational establishments are frequent targets. A pervasive lack of awareness about cyber security among employees and the general populace further increases system vulnerabilities. In this paper, a case study of Sarajevo Canton will be conducted, with the primary goal of highlighting, through real-world examples, all the deficiencies in the security system's response to cyber attacks.

Keywords: cyber security, cyber attacks, Bosnia and Herzegovina

1. Introduction

Cybersecurity has become a global priority, shaped by the growing threats and rapid technological advancements. This sector is characterized by diverse challenges, from high-profile ransomware attacks to the increasing demand for data access. The world is witnessing a series of significant cyber attacks that highlight the rising sophistication and scale of threats, leading to renewed efforts to create a secure and reliable cyber space (CSIS, 2024). These incidents underscore the importance of robust cybersecurity measures not only for individual companies or sectors but also for national infrastructure and global stability. According to insights from McKinsey, the rapid growth of on-demand data access and information platforms is expected to be one of the key trends impacting organizations and states worldwide in the next three to five years (www.mckinsey.com, 2023). This trend will significantly change how companies operate and how states manage their infrastructure, particularly in the context of cybersecurity.

[1] Contact address: jahic@fkn.unsa.ba

[2] Contact address: nhalilovic@fkn.unsa.ba

The Global Cybersecurity Report by the World Economic Forum also highlights the global implications of protecting electronic data and the cybersecurity concerns exacerbated by geopolitical fragmentation. These factors increasingly influence how companies operate and where they invest. Given the increasingly complex geopolitical relationships, protection against cyber threats is becoming crucial for maintaining stability on a global level (World Economic Forum, 2023). In light of these global trends, it is important for states and organizations to recognize the need for continuous investment in advanced cybersecurity measures. Building resilience against cyber attacks is becoming imperative not only for national security but also for economic growth and citizens' trust in digital services. In this context, international cooperation and alignment with global standards are key factors in creating a secure cyber space capable of responding to increasingly complex threats.

This paper analyzes the current state of cybersecurity in Bosnia and Herzegovina, with a particular focus on the legislative framework, cyber attack analysis, and potential avenues for improvement, in line with Bosnia and Herzegovina's aspirations for EU membership. Given the increasing digitalization of society and growing dependence on information technologies, the issue of cybersecurity becomes crucial for safeguarding national security, economic development, and the protection of citizens' privacy. The research highlights the urgent need for comprehensive cybersecurity legislation that would align with the EU Directive on Network and Information Security (NIS). The current legislative framework in Bosnia and Herzegovina, while existing, is not sufficiently developed or adapted to the modern challenges posed by sophisticated cyber attacks. Additionally, the absence of a unified national cybersecurity strategy further complicates coordination between different institutions and sectors.

Bosnia and Herzegovina faces numerous cyber attacks, including ransomware attacks, phishing campaigns, and DDoS attacks, which point to significant deficiencies in protecting critical infrastructure and IT systems. Cases show that state institutions, the financial sector, and educational institutions are frequent targets. Particularly concerning are attacks on critical infrastructure, which includes power grids, telecommunications, and financial systems, as these can have far-reaching consequences not only for state security but also for the daily lives of citizens. The lack of cybersecurity awareness among employees and the general population is an additional factor that increases system vulnerability. Education and raising awareness about the importance of cybersecurity are crucial for reducing the risk of attacks. Without proper training and preventive measures, the human factor remains the weakest link in the security chain, potentially leading to catastrophic consequences.

This paper will present a case study of the Canton of Sarajevo, with the primary goal of highlighting all deficiencies in the security system's response to cyber attacks through real-world examples. This approach will allow for the identification of specific problems and propose measures to overcome them, taking into account best practices from the EU and beyond. Given Bosnia and Herzegovina's aspirations for EU membership, adapting the national framework to the EU's requirements in the field of cybersecurity is of crucial importance for success on that path. Additionally, this paper provides an overview of the role of international cooperation, particularly with NATO and other European security organizations, in strengthening Bosnia and Herzegovina's capacity to defend against cyber threats. Regional cooperation is also important, as cyber threats often cross national borders and require a joint response. Through a comprehensive analysis, the paper aims not only to identify current

challenges but also to offer concrete recommendations for improving cybersecurity in Bosnia and Herzegovina, in line with global trends and standards.

2. Cybersecurity in Bosnia and Herzegovina - Analysis of the Current State

Cybersecurity is a crucial area for any country, encompassing a range of activities aimed at detecting, preventing, and responding to cyber-attacks, as well as protecting data and information from various threats, such as theft or compromise. „Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online" (NCSC, 2020). These threats can have severe consequences for national security, as well as the safety of organizations, communities, and individuals. Protection involves not only personal and health data but also sensitive information of all kinds, intellectual property, and data stored in government, business, and industrial computer systems. Developing an effective cybersecurity strategy is one of the most important steps toward preserving a country's security, protecting its information, and, ultimately, ensuring the safety of its citizens.

In the 21st century, cybersecurity has become an integral part of the functioning of a modern state, as was clearly demonstrated during the ransomware attack on Colonial Pipeline in the United States in May 2021. This incident targeted computer systems managing critical oil delivery infrastructure on the East Coast, causing serious disruptions and showing the extent of the threat cyber-attacks can pose to national security. In May 2021, Colonial Pipeline fell victim to a cyber-attack that led to a complete five-day shutdown. The attackers demanded a ransom of 75 bitcoins, equivalent to $4.4 million at the time, which Colonial Pipeline ultimately paid. Authorities managed to recover most of the ransom, but their further investigation revealed that the same attackers had received over $90 million in bitcoins from 47 different sources in the previous year (IFAC, 2022).

The consequences of cyber-attacks can be as devastating as those from traditional sources, highlighting the need for a strong and organized defense at the national level. The formation of CERTs (Computer Emergency Response Teams) becomes essential, especially in the context of increasing threats in the digital space. A CERT is a group of cybersecurity experts responsible for protecting, detecting, and responding to security incidents within an organization. The first CERT, established in 1988 at Carnegie Mellon University following the Morris worm incident, became a model for other teams worldwide. A CERT's role includes taking preventive measures before problems arise, detecting incidents using tools like intrusion detection systems, and responding to incidents to minimize damage and enable quick recovery. Their activities include employee training, developing security plans, and continuously monitoring and improving security systems (Sullivan, 2023).

In May 2022, NATO Deputy Secretary General Mircea Geoană warned of the possibility of massive cyber-attacks by Russia targeting key digital infrastructure in Georgia and Bosnia and Herzegovina, emphasizing that cyber-attacks, along with disinformation and digital espionage, are integral parts of modern warfare strategy. Although NATO promises to support countries in building their defense capacities against cyber threats, it remains unclear how aware institutions and organizations in Bosnia and Herzegovina are of the importance of these threats. It is still unknown to what extent formal exercises for cyber-attack scenarios are con-

ducted at the state level or what coordination mechanisms exist, if any. This raises questions about the security efforts undertaken by the Bosnian government to prevent cyber-attacks, mitigate potential damage, and protect critical infrastructure, businesses, and citizens' rights in a digital environment.

Given the above, it is crucial to reflect on the analyses of the current state conducted so far, which clearly demonstrate the deficiencies in the system. In Bosnia and Herzegovina, as in other parts of the country, we face serious challenges in the field of cybersecurity. Cyber risks, such as phishing attacks, ransomware, DDoS attacks, and other forms of cybercrime, have become significant threats to information security. Recent hacking attacks on key institutions like the Council of Ministers, the Parliamentary Assembly of BiH, and the Central Election Commission (CEC) are just a few examples of these risks. Data from the first report on cyber threats to members of the Parliamentary Assembly of BiH, prepared by the Cyber Security Excellence Center (CSEC) and the Balkan Investigative Reporting Network of Bosnia and Herzegovina (BIRN BiH), reveal that the country was exposed to nearly ten million cyber-attacks in a single month. These diverse attacks highlight the seriousness of the situation and the challenge posed by cyber threats. The report further emphasizes that Bosnia and Herzegovina suffers from a lack of key strategies, regulations, and capacities needed to effectively protect citizens, businesses, and institutions from cyber threats. Hacking attacks on institutions such as the Council of Ministers and the Parliamentary Assembly underscore the urgent need for a coordinated and responsible approach to addressing these challenges (BIRN, 2022).

Another report that confirms the previously presented situation comes from BIRN, and its title, "Bosnia and Herzegovina - A Complicated Legal and Administrative System Lagging in Recognizing Cybersecurity," hints at its findings. "Domestic legislation in BiH reflects the complex and decentralized structure of the country. Existing state-level legislation related to cybersecurity rarely and only partially addresses relevant issues. By signing international agreements and conventions, such as the Convention on Cybercrime and the Stabilization and Association Agreement, BiH is obligated to align its information and cybersecurity legislation with these instruments and establish enforcement mechanisms. However, the progress made so far in aligning in the field of cybersecurity has been insufficient," states the report (BIRN, 2023:5).

In addition to the challenges posed by the lack of a quality legislative framework and strategic documents regulating this area, a report titled "Cybersecurity in BiH: Progress, Potential and Unfinished Business" also points out that most institutions in Bosnia and Herzegovina lack a proactive approach to implementing information security management acts, resulting in weaker protection and low awareness of its importance (Jovanović and Brkan, 2023). The lack of coordination between institutions and agencies further complicates the fight against cyber threats and the efficient use of resources. Experts and NATO officials warn of the vulnerability of BiH and other Western Balkan states to cyber-attacks, particularly on critical infrastructure. The example of Montenegro in 2022 highlights the importance of international cooperation in recovering from such attacks. To best present the situation regarding the legislative framework, the next chapter will provide a closer description of the current state.

3. Legislative Framework

Bosnia and Herzegovina signed the Stabilization and Association Agreement with the European Union, committing to align its legislation with the EU acquis, including in the area of cybersecurity. The EU has adopted the Directive on Security of Network and Information

Systems (NIS Directive), which requires member states to strengthen cybersecurity capacities, ensure cross-border cooperation, and supervise critical sectors.

Although Bosnia and Herzegovina has laws related to cybersecurity, such as the Criminal Code and the Law on Personal Data Protection, they do not meet the specific requirements of the NIS Directive. At the entity level, the Republic of Srpska has adopted the Law on Information Security, but its implementation has not been fully carried out. Additionally, at the state level, BiH has yet to establish a CERT (Computer Emergency Response Team) for BiH institutions, although this was envisaged by the 2017 Decision.

For easier review, a tabular overview of the adopted laws related to cybersecurity according to the levels of government is provided below, starting with the state level of Bosnia and Herzegovina, followed by the lower administrative units, the entities of the Federation of Bosnia and Herzegovina and the Republic of Srpska, as well as the separate administrative unit of the Brčko District.

Table 1. Adopted Laws Partially Covering Cybersecurity by Level of Government

Level of government	Law
BOSNIA AND HERZEGOVINA	Criminal Code of Bosnia and Herzegovina Law on Criminal Procedure Law on Personal Data Protection Law on Protection of Classified Information Law on Communications of Bosnia and Herzegovina Law on Electronic Signature Law on Electronic Document of Bosnia and Herzegovina Law on the Prevention of Money Laundering and Financing of Terrorism Rulebook on Maintenance and Special Technical Measures for the Protection of Personal Data
FEDERATION OF BOSNIA AND HERZEGOVINA	Criminal Code of FBiH Law on Criminal Procedure of FBiH Law on Electronic Document of FB
REPUBLIC OF SRPSKA	Criminal Code of RS Law on Criminal Procedure of RS Law on Electronic Signature of RS Law on Electronic Document of RS Law on Electronic Business of RS Law on Information Security of RS
BRČKO DISTRICT	Criminal Code of Brčko District Law on Criminal Procedure Instruction on the Method of Executing Protection of Classified Information on Computers

The legal framework in Bosnia and Herzegovina reflects the complex nature of the country. While there are laws concerning cybersecurity at both the state and entity levels, they do not cover all relevant aspects. Bosnia and Herzegovina is obligated to align its legislation with international agreements and conventions, including the Convention on Cybercrime and the Stabilization and Association Agreement. Currently, progress in this area is limited, although the Council of Ministers of BiH approved the establishment of a CERT team within the Ministry of Security in May 2023. A key challenge remains the lack of a national cybersecurity strategy.

4. Cybersecurity in Sarajevo Canton – A Case Study

In the context of increasing digitalization of society, Bosnia and Herzegovina, including its capital Sarajevo, is not exempt from the growing threat of cyberattacks. These attacks, which have become an integral part of modern security challenges, require a deeper understanding in order to develop adequate protection strategies. Analyzing the history of cyberattacks in Bosnia and Herzegovina, particularly in Sarajevo, provides insight into the evolution of these threats and examines how authorities and organizations have responded to the challenge of security in a digital environment.

4.1. Overview of Cyberattacks in Sarajevo Canton

The following section presents three of the most recent cases of cyberattacks directly targeting state institutions located in Sarajevo Canton, as well as lower levels of government and companies representing the city's critical infrastructure.

In August 2020, police officers from the Department for Combating Computer Crime of the Federal Police Administration, in cooperation with the Sarajevo Canton Prosecutor's Office and Europol, identified a suspect for the criminal offense of "Damaging Computer Data and Programs." According to the Federal Police Administration, the suspect, an Iranian national, used information technology skills and anti-forensic measures to carry out a hacking attack on the information system of the Municipality of Centar Sarajevo and "UTIC" Sarajevo on June 5 and 6, 2020. The suspect utilized virtual private networks (VPNs) and virtual private servers (VPSs) located in France, Germany, the Netherlands, and Finland to hide his actual location and connected to the internet via the IRANCELL-NET operator from Tehran. Exploiting vulnerabilities in the Municipality of Centar Sarajevo's system, he unauthorizedly installed the malicious program "Sorena" for data encryption, subsequently demanding ransom for decryption. A day later, on June 6, 2020, he launched a similar attack on the UTIC Sarajevo system using the "Mamba" program, which paralyzed the system's operations (N1 BiH, 2020). These attacks caused significant material damage, primarily in terms of the time required to restore the system and operational delays in the municipality, particularly in the issuance of building permits. The Federal Police Administration submitted a report to the Sarajevo Canton Prosecutor's Office and notified the Iranian authorities through Interpol for further action against the suspect.

A cryptolocker, a type of cyberattack, involves locking a company's data with the aim of extorting money. In September 2022, such an attack was recorded at the company Sarajevogas, which successfully protected its data thanks to appropriate security measures. Inspector Saša Petrović from the Cybercrime Department of the Federal Police Administration

emphasizes that cyberattacks are "complex, difficult to detect, and have a serious impact on business data" (TV SA, 2022). Cyberattacks are becoming increasingly common in Bosnia and Herzegovina, as well as globally, with numerous reports from citizens and companies. Different motives and methods of cybercrime highlight the complexity of the problem, while the lack of comprehensive legislation makes it difficult to combat these threats. Although technology is advancing rapidly, the legislative framework for cybersecurity often lags behind. Bosnia and Herzegovina faces the absence of a comprehensive national cybersecurity strategy, inadequately defined critical infrastructure, and the lack of legal recognition of cryptocurrencies like Bitcoin, which further complicates the fight against cyber threats. Experts warn that cyberattacks will continue to be a threat in the future, and investment in the protection of information systems is essential. Recently, the Intelligence and Security Agency of BiH called on institutions and the private sector to check the security of their systems and take appropriate preventive measures. "We advise all individuals and organizations to conduct a security assessment of information and communication systems and apply security measures as soon as possible to proactively prevent potential 'cyber' attacks in Bosnia and Herzegovina," states an official announcement published shortly after the attack on Sarajevogas (Al Jazeera Balkans, 2022).

Additionally, a hacking attack that disabled the website of the Parliamentary Assembly of Bosnia and Herzegovina highlighted the risks of cyberattacks on the country's IT systems. Although the nature of the attack on the Parliament server is still unknown, informal reports suggest it was a Crypto Locker attack that locks down the entire system. The State Investigation and Protection Agency (SIPA) took all necessary measures, and the case was forwarded to the BiH Prosecutor's Office for further investigation and protection of cybersecurity of state institutions. After the attack in September 2022, computers in the buildings of the Parliament and the Council of Ministers became practically unusable. Still, aside from their experts, these institutions had no other state specialized agency to turn to. Despite years of calls from the European Union and other international partners, BiH has never formed a Computer Emergency Response Team (CERT). Representative Zlatko Miletić confirmed to BIRN BiH that the computers and internet connection were restored after the attack, but he does not know how it was done. "Who, how it was repaired, I really do not know at this moment," says Miletić. He adds that just a few days after the consequences of the September cyberattack were repaired, there were additional attempts to breach the system (Hodžić, 2022).

4.2. Overview of Official Statistics from the Sarajevo Canton Ministry of Internal Affairs

This section will present the results of an investigation into reported criminal offenses against electronic data processing systems from 2020 to 2023, along with their analysis and discussion. The data presented is obtained from the official records of the Department for Economic Crime and Anti-Corruption of the Criminal Investigation Sector of the Sarajevo Canton Ministry of Internal Affairs.

During the four-year period from 2020 to 2023, the Department for Economic Crime and Anti-Corruption of the Criminal Investigation Sector of the Sarajevo Canton Police Administration recorded numerous reports of criminal offenses against electronic data processing systems under Chapter XXXII of the Criminal Code of the Federation of Bosnia and Herzegovina. The collected data provides insight into the dynamics of reported criminal offenses and the effectiveness of the judicial system in addressing them. The following table

presents data on the number of reports of criminal offenses against electronic data processing systems for each year from 2020 to 2023.

Table 2. Number of Reports of Criminal Offenses Against Electronic Data Processing Systems (2020-2023)

Year	Number of Reports
2020	34
2021	54
2022	24
2023	33

In 2020, there were a total of 34 reports of criminal offenses against electronic data processing systems. This year marks the beginning of the analyzed four-year data series and is characterized by a moderate number of reports. However, it is noteworthy that none of these cases were resolved, indicating initial challenges in investigating and prosecuting cybercrime. Table 3 shows the number of resolved cases for the same period.

Table 3. Number of Resolved Criminal Cases Against Electronic Data Processing Systems (2020-2023)

Year	Number of Resolved Cases
2020	0
2021	3
2022	0
2023	15

In the following year, 2021, there was a significant increase in the number of reports, with a total of 54 reported cases. This increase may indicate greater awareness of cybercrime or a real rise in incidents in this sector. However, only three of the reported cases were resolved, suggesting challenges in investigative processes and the effectiveness of the judicial system.

In 2022, the number of reports decreased to 24 cases. This decrease may result from various factors, including potential changes in strategies or prioritization of cybercrime

by relevant institutions. However, despite the lower number of reports, the resolution rate remained zero, highlighting ongoing challenges in prosecuting cybercrime.

In 2023, the number of reports increased again to 33 cases. This trend of rising reports may indicate the persistence of cyber security threats or increased awareness of these threats in the community. Notably, this year saw 15 of the reported cases resolved, representing a significant improvement compared to previous years.

The data reveals certain trends and fluctuations in the number of reports and resolved criminal cases over the four-year period. The number of reports varies from year to year, while the effectiveness in resolving these reports also changes. The analysis of the collected data on reports of criminal offenses against electronic data processing systems under Chapter XXXII of the Criminal Code of the Federation of Bosnia and Herzegovina for the period from 2020 to 2023 provides insights into the dynamics of cybercrime incidents. The year 2021 stands out with the highest number of reported cases, which may indicate increased activity by cybercriminals or improved public awareness of these threats. Conversely, 2020 and 2022 show a lower number of reports, which could result from various factors such as changes in attacker strategies or changes in the priorities of relevant authorities in combating cybercrime. It is important to note that, despite fluctuations in the number of reports, the effectiveness of the judicial system in resolving these cases is not consistent. The years 2020 and 2022 recorded no resolutions for reported cases, while 2021 had a low resolution rate. It was only in 2023, with a significant increase in resolved cases, that noticeable progress in this segment was observed.

The analysis of the collected data provides insight into the complexity of the cybercrime problem and the challenges faced by relevant institutions. Zero resolution of criminal offenses in 2020 and 2022 may indicate a lack of adequate resources or effective investigative procedures during those years. This may include a lack of trained personnel, specialized equipment, or technology needed for successfully addressing cybercrime. To improve the situation, it is essential for relevant institutions to work on enhancing their capacities and procedures. This includes strengthening resources such as staff training, investing in specialized equipment and technology, and improving coordination between police teams, judicial authorities, and other relevant agencies. Additionally, the adoption and implementation of adequate laws and strategies are crucial for strengthening the cyber risk management system and combating cybercrime.

Conclusion

The analysis of cybersecurity in Bosnia and Herzegovina, with a specific focus on the Sarajevo Canton, reveals significant vulnerabilities within the country's digital infrastructure, legislative framework, and institutional preparedness to counter cyber threats. The increasing number and complexity of cyber attacks, including ransomware and phishing campaigns targeting state institutions and critical infrastructure, underscore the urgent need for a comprehensive cybersecurity strategy and robust legal frameworks aligned with EU standards. The current fragmented and insufficiently developed legislative environment, coupled with the absence of a national Computer Emergency Response Team (CERT) and lack of effective coordination mechanisms, hampers the country's ability to respond to evolving cyber threats.

Moreover, low awareness of cybersecurity measures among employees and the general population further exacerbates vulnerabilities.

The case study of the Sarajevo Canton demonstrates the real-world impact of cyber attacks and highlights significant gaps in response and recovery mechanisms. The data shows an inconsistent and generally low rate of resolving reported cybercrime cases, indicating a need for better resources, training, and strategic coordination among law enforcement and security agencies. To address these challenges, Bosnia and Herzegovina must prioritize the establishment of a unified national cybersecurity strategy, invest in capacity building, foster international cooperation, and align its legislative framework with global cybersecurity standards. Strengthening these areas is not only crucial for national security but also essential for economic stability and achieving the country's aspirations for EU membership.

Literature

- BIRN (2022). Izvještaj o CYBER SIGURNOSNIM PRIJETNJAMA u Bosni i Hercegovini. Available at: https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-BOS-WEB.pdf [Accessed 28 Aug. 2024].
- Hodžić, E. (2022). BiH ranjiva na cyber napade zbog nedostatka ključnih dokumenata. Available at: https://detektor.ba/2022/11/14/bih-ranjiva-na-cyber-napade-zbog-nedostatka-kljucnih-dokumenata/ [Accessed 28 Aug. 2024].
- IFAC (2022). SPREČAVANJE PRANJA NOVCA: OSNOVE Dio 7: Virtualna imovina. Available at: https://www.srr-fbih.org/sites/default/files/standards/2023-10/Osnove%3A%20Spre%C4%8Davanje%20pranja%20novca%2C%20Dio%20sedmi%3A%20Virtualna%20imovina.pdf.
- Jovanović, M. and Brkan, D. (2023). Policy Brief: Cybersecurity in BiH: Progress, Potential and Unfinished Business. UG Zašto ne. Available at: https://zastone.ba/app/uploads/2023/06/Cybersecurity-in-BiH-Progress-Potential-and-Unfinished-Business-1.pdf.
- McKinsey & Company (2023). What is cybersecurity? Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity#/.
- N1 BiH (2020). FUP: Iranac hakerski napao Općinu Centar Sarajevo. Available at: https://n1info.ba/vijesti/a455126-fup-iranac-hakerski-napao-opcinu-centar-sarajevo/ [Accessed 28 Aug. 2024].
- NCSC (2020). What is cyber security? [online] ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.
- Sullivan, P. (2023). What is CERT? WhatIs.com. Available at: https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team.
- TVSA Sarajevo (2022). Dnevnik TVSA/ Cyber napad na 'Sarajevogas'. Available at: https://www.tvsa.ba/dnevnik-tvsa-cyber-napad-na-sarajevogas/ [Accessed 28 Aug. 2024].
- World Economic Forum (2023). Global Cybersecurity Outlook 2023. Available at: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.