Policy brief

Cybersecurity in BiH: Progress, Potential and Unfinished Business

Publisher: UG Zašto ne

Authors: Milan Jovanović, Darko Brkan

Sarajevo, June 2023

1. Executive Summary

Despite the rising global cyber-attack rates[1], Bosnia and Herzegovina still lacks a cybersecurity strategy, although some strategies at various levels in BiH partially deal with the cybersecurity issue. BiH is the only country in the Western Balkans without such measures for combating cyberspace threats.[2]

According to the results of Surfshark's research on the quality of digital well-being, Bosnia and Herzegovina is in 80th place out of 117 countries included in the study[3]. At the same time, it holds 110th place on the ITU Global Cyber Index, which makes it the worst-ranked regional state.[4]

The European Commission noted the lack of a comprehensive strategic approach as early as 2016, stating that Bosnia and Herzegovina's response to cyber security threats was inadequate.[5]

There is no official data on the number and type of cyberattacks. Unofficial information indicate that BiH's cyberattacks have increased by 1300 times weekly. Out of 68 institutions of BiH, 24 institutions of BiH had recorded cyber-attacks.[6]

There is a significant delay in establishing the CERT for BiH institutions in relation to the defined deadline. It was only in May 2023, six years after the initial decision of the Council of Ministers, that the conditions for establishing that body were met, although several other CERT teams function at the entity and institutional level.

As of now, the academic Cyber Security Excellence Centre is the only functional and operational CERT covering BiH territory, dealing in threat analytics, information sharing, incident response and giving advice and support.

Between November 17 and December 17 last year, Bosnia and Herzegovina faced over 9.2 million cyber threats, mainly DDoS attacks.[7] The vulnerability of citizens, businesses, and crucial sectors like law, economy, energy, health, and education to cyberattacks was highlighted in the recent audit report by the Audit Office of Institutions in Bosnia and Herzegovina.[8]

As a result of the postponement, there is yet no guarantee for a synchronized strategy in handling cyber breaches. The lack of legislation and strategic framework, inadequate coordination and the lack of awareness across the whole society renders BiH society open to cyber threats and block both proactive and reactive cybersecurity measures from being implemented across Bosnia and Herzegovina's institutions.

NATO representatives and experts are increasingly worried about the susceptibility of Western Balkan nations, Bosnia and Herzegovina included, to cyber threats, particularly those targeting crucial systems, originating from nations such as Russia.

Although there are several[9] international efforts[10] and positive initiatives to help build BiH's cyber capacity, establishing a functioning state-level CERT and cyber strategy for BiH in today's interconnected world is essential as the consequences of cyber-attacks can be severe, with potential impacts on national security, economy, infrastructure, and public trust.

To overcome the issues, BiH should develop Cybersecurity Strategy, establish a CERT for BiH institutions, work on facilitating and promoting public-private partnerships, work on regional and international cooperation, invest in IT infrastructure and implement an awareness campaign on the importance of cybersecurity at all levels of the society.

2. Background

The ITU (International Telecommunication Union) definition states that cybersecurity includes a set of tools, security concepts, protective measures, and training and technology that can be used to protect the cyber environment.[11]. Any network-connected technology can be a potential target, and protecting users and devices is challenging. This protection extends to personal and health data, sensitive data, intellectual property, and information in governmental, business, and industrial systems. Cybersecurity strategy is one of the most important tools for preserving the security of a country, its data, and its citizens.[12]

The high positioning of cyber security on the international level is also evidenced by the fact that in 2016, member states at the NATO Summit in Warsaw recognized cyberspace as the fourth domain of operations within which states must defend themselves effectively, just as they do in the air, on land, and at sea.[13]

Cybersecurity has become a critical concern globally, shaped by both emerging threats and evolving technologies. Diverse challenges characterize the landscape, from high-profile ransomware attacks to the growing demand for ubiquitous data access. Around the world, we are witnessing a series of notable cyber-attacks that highlight the increasing sophistication and scale of threats, leading to renewed efforts to create a safe and trustworthy cyberspace.[14] These incidents underscore the importance of solid cybersecurity measures for individual businesses or sectors, national infrastructure, and global stability.

McKinsey's insights[15] suggest that in the next three to five years, the rapid growth of on-demand access to ubiquitous data and information platforms will be one of the significant trends impacting organizations and countries worldwide. The World Economic Forum's Global Cybersecurity Outlook also underscores the global implications of e-data protection and cybersecurity concerns created by geopolitical fragmentation, as these factors increasingly influence how businesses operate and the countries in which they invest.[16]

The fast development of publicly available Artificial Intelligence (AI) solutions has significantly transformed the cybersecurity landscape, strengthening defenses but also empowering malicious actors and introducing threats like AI-powered deepfakes, potentially undermining trust in digital communications. As AI advances, the cybersecurity landscape will likely continue to evolve, demanding ongoing vigilance, adaptation, and innovation.

Balkan states are increasingly susceptible to cyberattacks due to inadequate preparation, with countries like Bosnia unable to combat millions of monthly cyberattacks. Recent widespread cyberattacks, including those on Montenegro and Albania in 2022, emphasize the urgent need for enhanced regional cybersecurity measures. The growing threat of cyberattacks highlights the need to improve regional cybersecurity infrastructure and capabilities to protect their digital assets and information.[17]

3. Policy Issues Addressed

Last year, in just one month, from November 17 to December 17, Bosnia and Herzegovina saw more than 9.2 million cyber security threats, most of which were DDoS and came from Brazil, the Netherlands, and the USA according to the Bosnia and Herzegovina Cyber Security Threat Assessment Report.[18] The most effective illustration of how vulnerable citizens, businesses, and institutions in BiH are to cyberattacks that could jeopardize important sectors like the rule of law, the economy, energy, health, or education is portrayed in the most recent audit report by the Audit Office of the Institutions in Bosnia And Herzegovina.[19] The report states that BiH's institutions have taken a relatively passive approach to implementing information security management practices. Only 14 of the 68 institutions have information security management actions in place that are in accordance with the Information Security Management Policy.

Just in May 2023, six years after the decision of the Council of Ministers[20], functional conditions were created for the work of the Computer Incident Response Team (CERT) for bodies and institutions of Bosnia and Herzegovina, per the recommendations of the European Commission.

Still, responsible institutions in BiH have failed to implement a strategic and legislative cybersecurity framework to organize and manage responses to computer incidents properly. The repercussions of failing to meet fundamental cybersecurity criteria harm public administration operations and may result in data misuse and financial resources critical to the country's running and citizens' daily lives.

3.1 Insufficient legislation and strategic framework

The legal framework in BiH reflects the complex nature of the country. Although there are cybersecurity laws at the state and entity levels, they do not comprehensively cover all relevant matters. BiH has committed to adopting international agreements and conventions, such as the Convention on Cybercrime and Stabilization and Association Agreement, which mandates that its information security legislation is consistent with these frameworks. The most significant regulations related to cybersecurity at the EU level are the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), adopted in 2023 (replacing the NIS1 Directive), and the EU Cybersecurity Act, adopted in 2019.

Unfortunately, there have been limited advancements toward achieving alignment in this area so far. EC 2022 Report on Bosnia and Herzegovina emphasizes the need for further alignment on cybercrime with the EU *acquis* and calls for the completion of the strategic framework on fighting cybercrime, as the strategy is only in place in the Republic of Srpska entity. [21]

Recent hacker attacks on the BiH’s institutions as well as the new cyber security threat assessment done by CSEC and BIRN BiH probably prompted the relevant institutions to act. The Council of Ministers approved in May 2023 the amendments to the Rulebook on the Internal Organization of the Ministry of Security of BiH, which allows the establishment of a CERT within the Ministry of Security.[22] This move could represent a start of a systemic response in solving the issue of cybercrime and security threats in BiH institutions, both in the fight against cyberattacks on BiH institutions and in aligning BiH with the EU acquis and strategic documents on cybersecurity.

The Ministry of Security of Bosnia and Herzegovina have informed us that they will, as soon as legal conditions are met, initiate the process of admitting staff into the CERT as well as creating a comprehensive Plan for operational and institutional establishment of the CERT and achieving the goals of CERT (coordination and cooperation with relevant bodies in BiH, elimination and reduction of consequences of security incidents caused by unauthorized intrusion into ICT systems in BiH institutions, improving the reliability of ICT systems in BiH institutions through constant dedication, work on prevention and minimization of the possibility of security incidents, assisting administrators in implementing proactive measures to reduce the risk of security incidents, assisting in preventing the consequences of security incidents, etc.). Also, the plan is to join international CERT associations, organizations, and networks, which will provide BiH with the opportunity to exchange information related to current cyber threats and attacks as well as best practices and recommendations for protecting the IT systems of BiH institutions.

The initial steps in building cybersecurity were achieved by signing the Convention on Cybercrime in 2006 and the Stabilization and Association Agreement in 2008. Efforts to implement a strategic and legal framework for cybersecurity were initiated in 2017, but only now, after six years, these activities seem to be moving from ground zero.

According to the Constitution, BiH consists of two entities, the Federation of BiH (FBiH) and the Republic of Srpska (RS), which have their own criminal laws and laws on criminal procedure. The Brčko District is a separate self-governing administrative unit with its own criminal laws. The legal provisions of the Brčko District related to cybersecurity and cybercrime are the same as those specified in the Criminal Code of FBiH. Above these laws, at the state level, there is the Criminal Code of BiH. However, it does not deal with specific issues related to cybersecurity, which are relegated to the level of criminal legislation in the three parts of the country.[23]

Currently, at the institutional level, eight laws in force contain provisions related to internet security or network security. Still, no law exclusively deals with the issue of cybersecurity.[24] With the help and support of UNDP, the Law on Network,and Information Security in the institutions of Bosnia and Herzegovina has been drafted and is currently in the phase of collecting opinions.[25]

In December 2022, the Government of the Federation of Bosnia and Herzegovina (FBiH), on the Federal Ministry of Transport and Communications proposal, determined the Draft Law on Information Security of FBiH and submitted it to parliamentary procedure. This Law regulates the field of information, or cybersecurity, in the Federation of Bosnia and Herzegovina for the first time.[26]The Republic of Srpska adopted the Information Security Law in 2011[27], establishing measures and standards for ensuring information security, dealing with data protection within the entity government, and designing bodies to adapt, implement, and monitor relevant measures.

With the adoption of the Law, the CERT RS was also established, which serves as the national CERT of the Republic of Srpska, and became operational in 2015. This was followed by Law on the Safety of Critical Infrastructures in 2019 and a strategy for the fight against cybercrime (2019-2023). As was noted by a PWC report, the baseline structure of the current cybersecurity framework in RS is generally in line with EU principles.

Despite these measures, the 2022 PWC report revealed that the Republic of Srpska suffered approximately ₤35 million in financial losses due to cyber incidents. Aside from the rising ransomware attacks aimed at small and medium-sized enterprises, there is also a rise in sophisticated Distributed Denial-of-Service attacks aimed at media outlets, healthcare websites, and other portals. The entity is also witnessing a steady increase in cybercrime, with 96 criminal acts recorded in 2019, and growing to 190 in 2020. In the first couple of months of 2021, this number was already at 115. The Federation of Bosnia and Herzegovina reports an approximate average daily occurrence of five cyberattacks leading to around £1 million worth of annual losses caused by such breaches.

From the Federal Police Administration, we were told that they believed that Bosnia and Herzegovina is not under greater danger than that which threatens other states in the region and Europe. They stressed that for better protection of critical infrastructure, BiH needs to adopt a national strategy for network security, aligning its laws with EU's NIS directives. We've been informed of DDoS, BEC, CEO, and ransomware attacks on critical infrastructure, often targeting large companies. The specifics of these attacks weren't disclosed. The number of cyber-attacks is typically correlated with other traditional crimes, making accurate statistics difficult. The financial damage from these attacks averages at 100,000 KM, often due to lacking security policies.

Recently, the Intelligence-Security Agency in BiH (OSA BiH) issued a warning to individuals, institutions, and the private sector that cyber-attacks seem to be becoming more frequent. It is not specified what kind of attacks they are, and with what purpose. But it was requested that preventive protection measures be taken. The Federal Police Administration (FUP) says they receive reports of cyber-attacks daily. And the target of attacks, most often, at least for now, are not citizens.[28]

CYBERSECURITY IN BIH

Adopted documents	Required documents
• Budapest Convention on Cybercrime	• Strategy on Cybersecurity in BiH
• Strategy for Establishment of BiH CERT	• Law on Organization and competencies of state bodies for countering cybercrime
• Strategy for the Prevention of and fight against Terrorism 2015-2020	• Law on Information Security in BiH (the draft law is currently in the phase of gathering opinions)
• Information Security Management Policy in BiH institutions (2017-2022)	Law on Information Security in FBiH (currently in the parliamentary procedure)
• Decision designating CERT for the institutions of BiH	• Law on the protection of critical infrastructure in BiH and FBiH
• Analyses on (non)compliance of legal regulations in cybersecurity field in BiH	
• **Rulebook on the Internal Organization of the Ministry of Security of BiH**	

(*Adopted and required legal framework, source: BiH Cybersecurity Threat Assessment March 2023)*[29]

Although some documents related to cyber security have been approved, and there is progress on establishing a CERT for BiH bodies and institutions, there is still a considerable distance to cover. The absence of a state strategy in this area is the biggest obstacle in creating a whole series of documents and laws that could ensure the cyber security of the citizens of BiH. Additionally, it's essential to reinforce the proficiency of professionals in the fields of information technology and communication.

3.2.Lack of awareness

In Bosnia and Herzegovina, most institutions lack a proactive stance towards implementing information security management acts. While an Information Security Management Policy exists, it remains unknown to some, while others consider their operations exempt from its requirements. The Ministries of Communications and Transport, and Security haven't effectively monitored its application or raised awareness about it, resulting in insufficient cybersecurity protection and a lower appreciation for its importance, affecting operational safety and efficiency.[30]

Experts[31] and NATO officials[32] express concerns about the vulnerability of Western Balkan states, including Bosnia and Herzegovina, to cyber-attacks, especially on critical infrastructure, by countries like Russia. Some believe these countries couldn't protect themselves against cyber warfare-capable nations. The 2022 cyber-attacks on Montenegro's government, resulting from lack of preparedness and awareness, underline these concerns. However, this case also emphasized the vital role of international cooperation and assistance in recovery from such attacks.

Some reports suggest an overall lack of awareness and understanding of the possible threats – a lack of ICT literacy among the citizens as well. This makes individuals and organizations more vulnerable to cyber-attacks.[33]

3.3. Inadequate coordination:

Currently, there is a lack of coordination between government institutions, law enforcement agencies, and other stakeholders involved in cybersecurity efforts, as concluded in the OSCE report.[34] This can lead to duplication of efforts and ineffective use of resources.

According to available information, the CERT of the Republic of Srpska was established in BiH in 2015. Cyber Security Excellence Centre, the academic CERT in Sarajevo, was established in June 2022 in collaboration with the University of Sarajevo, whose goal is to primarily provide services to the academic community, independent media organizations, and civil society organizations (CSOs) across the country. The CSEC's academic origin, provides the opportunity to combine expertise and experience, building links with the private sector and ultimately supporting the cybersecurity workforce development in B&H.

The Ministry of Defence has an operational CERT and has developed its own cyber defense strategy to establish a secure cyber environment for the information systems within its Ministry only. The Draft Law on Information Security of FBiH also envisages the establishment of a CERT team for FBIH. In May 2023, the Council of Ministers of BiH approved the Proposal for the Rulebook on Amendments to the Rulebook on the Internal Organization of the Ministry of Security of BiH, which creates conditions for the establishment of CERT for bodies and institutions of Bosnia and Herzegovina, that will lead to a central competent authority facilitating communication between already existing CERT bodies and data aggregation on national, entity, district, and cantonal level.

3.4. International support and cooperation

While formal cooperation channels are not established at the national level yet, there has been significant engagement between relevant parties in recent years. This interaction has occurred through various activities such as events, training sessions, and national and regional conferences. Key stakeholders, including UNDP, OSCE, and USAID, have provided international support alongside the EU Delegation to Bosnia and Herzegovina, which has played a crucial role in assisting with the implementation of the NIS Directive, establishing connections with ENISA, and enhancing existing capabilities.[35]

The government of the Federal Republic of Germany has funded a three-year project, "Building Cybersecurity in Bosnia and Herzegovina" implemented by the United Nations Development Programme (UNDP), which began in late 2022 and aims to strengthen the country's cybersecurity framework and improve the skills of cybersecurity professionals.[36]

According to publicly available information, the country has only several international agreements that contain cyber aspects, focused primarily on police cooperation and the fight against cybercrime. These include agreements with the Czech Republic, Saudi Arabia, and Ukraine. There are also two international cooperation documents on ICT, with Croatia and Turkey. [37]

China has been actively collaborating with various channels. In 2018, at the Third China-Central and Eastern European Countries (CEEC) Innovation Cooperation Conference in Sarajevo, Bosnia and Herzegovina's Ministry of Communications and Transport signed a deal with Huawei for technical support to the 'Smart City' and 'Safe City' projects. [38] However, this could potentially impede BiH's NATO aspirations due to security concerns and transparency issues related to Huawei and Chinese hardware.

Over the past decade, numerous activities have been conducted in Bosnia and Herzegovina under NATO's Science for Peace and Security Programme, spanning areas like cyber defense, counter-terrorism, and explosive risk identification, in collaboration with experts from NATO and partner nations. [39] In 2023, the Alliance also provided BiH with a support package, including nine aid projects for the defense system and three for the security system, as per BiH high officials. [40]

According to the publicly available reports, a Protocol on Cooperation between the Republic of Srpska and the Police Department of Moscow in 2016. The agreement encompasses cooperation in the areas of the fight against terrorism, arms, and drug trafficking, but also cooperation in cybercrime and training in various segments.[41] On the other hand, in May 2021, a Memorandum of Understanding was signed between the representatives of the Republic of Srpska and an Israeli company *Elta Systems*, to establish a Cyber Academy in Banja Luka.[42] According to some reports, 6.2 million BAM (3.2 million EUR) will be invested in this project by the end of 2025.[43]

4. Policy Options & Recommendations

4.1. Development of a Cyber Security Strategy for BiH: Establishing a comprehensive strategy is fundamental for enhancing cybersecurity. The strategy should outline key priorities, actions, and collaborations needed with various stakeholders, including government bodies, businesses, and individuals to safeguard national security, economic prosperity, and maintain the integrity of digital services. The strategy needs regular reviews and updates to keep up with the changing cyber threat landscape, preventing BiH from falling behind amid escalating cyber-attacks.

Predrag Puharić, CSEC CEO, told us that as much as 80 percent of the Guidelines for a strategic cybersecurity framework in BiH, produced by Neretva, an informal working group which functions under the auspices of the OSCE Mission in BiH could serve as a solid base for the Strategy.

In that regard, both Neretva and CSEC could work together to update the document and facilitate the process of developing the document.

Legislatively, the penal code should be updated to recognize various forms of cyber-criminal acts like cyberbullying or revenge porn.

4.2. Establishment of a CERT for BiH bodies and institutions: After the preconditions have been fulfilled, a central CERT should be established within the Ministry of Security as soon as possible to oversee and coordinate efforts across different sectors and serve as a point of contact for international cooperation. The processes should be transparent, with clearly defined roles and responsibilities. After its establishment, it is imperative to allocate appropriate financial and human resources to the CERT to respond to cyber incidents at a national level effectively.

4.3. Public-Private Partnerships: Given the public sector's limited capacity to tackle major cyber-attacks alone, there's a growing acknowledgement of the need for increased collaboration between public and private entities in cybersecurity. This could boost national resilience against such threats, possibly through short-term outsourcing of cybersecurity services to address current institutional gaps. Businesses, particularly in tech, often have the latest tools, specialized knowledge, and hands-on experience to counter cyber threats. Government bodies can provide legal tools, international collaboration access, policy support, and resources for training and research. Civil society, media, and digital security professionals could focus on raising public awareness. This symbiosis is increasingly vital given the quick evolution of cyber threats and growing global reliance on digital infrastructure.

4.4. Regional and International Cooperation: As cyber threats are global, international collaboration is essential for an effective response. Enhancing communication and cooperation among all regional players is key to building necessary resilience. Bosnia and Herzegovina could strive for closer collaboration with other countries and international organizations like the European Union, United Nations, and more. Given expert predictions of ongoing threats and cyber-attacks in the Western Balkans region, there's an increasing need for enhanced regional cooperation and information exchange. Montenegro, which received considerable international aid and expertise following cyber-attacks in August 2022, could be a useful source of best practices and procedural development.

4.5. Capacity Building and Education: Capacity building and education are crucial in cybersecurity, fostering a knowledgeable and resilient digital community. Given the swift evolution of cybersecurity threats in our digital-dependent world, continuous learning and adaptation are necessary. Global cybersecurity firms report that over 90% of successful attacks begin with emails, the most common attack vector. To address this, BiH institutions could create training programs to bridge the technical personnel gap in the short term and strengthen public administration employees' knowledge. A competence center for BiH could be established in the mid-term as a knowledge hub for information sharing and skill development, serving the private sector, interested public, and academia. [44] As no master or specialist programs focusing on cybersecurity education were identified in the entire Western Balkans by the Cybersecurity Capacity Review report[45], establishing cybersecurity curricula at all education levels is necessary. This would foster the development of future cybersecurity professionals, essential for the digital world.

4.6. Public Awareness Campaigns: There is a pressing need for a comprehensive awareness campaign on cybersecurity, targeting all societal segments. Given the escalating cybercrime threats, enhancing public understanding of cybersecurity is crucial for the protection of institutions, organizations, and individuals in BiH, fostering resilience. This involves educating the public about various cyberattacks, such as phishing, malware, ransomware, and data breaches, and their potential repercussions. An informed individual is less likely to fall prey to these threats, being better equipped to recognize and respond to suspicious online activities. Accordingly, institutions should consider a baseline cybersecurity program for all public sector employees and foster openness to public and media communication, enhancing public service. This can be achieved in collaboration with CSOs and cybersecurity experts, enabling the identification of vulnerable public groups, such as children with high online presence. Partnering with the media can also be fruitful, as they can distribute manuals, PDFs, and information on good cybersecurity practices accessible to everyone.

4.7. Investment in Infrastructure and Technology: BiH must allocate adequate funds to acquire and maintain essential cybersecurity infrastructure and technologies, spanning both preventive measures like firewalls and intrusion detection systems, and responsive tools for incident handling. Such investment facilitates the development of secure digital landscapes, incorporating the creation and deployment of secure servers, databases, network equipment, and the implementation of security protocols. Additionally, the growing role of innovative technologies like AI and machine learning in the cybersecurity domain can't be overlooked. These technologies enable automated threat detection and response, curtailing the time taken to counteract an attack, thereby limiting potential harm. This investment would empower state institutions to establish a more secure environment, adopt a proactive stance to cybersecurity utilizing AI solutions, and adapt to emerging threats.

5. Conclusion

Due to the lack of an agreed strategic framework for cyber security, Bosnia and Herzegovina is lagging in fulfilling its obligations and regulating the field of cyber security, which has damaged the institution and the country's reputation. The lack of a strategic framework also entails a lack of legal solutions.

In the absence of a strong framework, security warnings and international recommendations for responding to cyber incidents have not been fully met, which is why the information and network systems of BiH institutions are more susceptible to cyber threats.

Expert-wise, the global shortage of cybersecurity experts is arguably felt even more strongly in BiH, with the ongoing trend of high emigration from the region. Also, a general lack of awareness of cyber risks and threats across all parts of society is one of the key obstacles to building a more resilient country. This is why a multistakeholder and multilevel approach is essential.

Fulfilling the conditions for forming a CERT for BiH institutions is a good step forward, despite the significant delay. In any case, the state must ensure the conditions for the smooth establishment and operational activities of CERT, as well as the connection with already existing teams, for the sake of data centralization and analysis, records of cyber incidents, and the exchange of information, security recommendations, and expertise.

Despite various international actions and beneficial programs to strengthen BiH's cybersecurity capabilities, creating an operational CERT at the state level and a comprehensive strategy is paramount in our current interconnected society. Cyber-attacks' ramifications can be drastic, potentially affecting national security, the economy, infrastructure, and the public's confidence.

6. References

[11] https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/#:~:text=The%20Top%20Cybersecurity%20Statistics%20of%202023%20(So%20Far),-There%20are%20an&text=An%20estimated%202%2C200%20cyberattacks%20per,first%20half%20of%202022%20alone

[2] https://detektor.ba/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/?lang=en

[3] https://surfshark.com/dql2022?country=BA

[4] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[5] https://neighbourhood-enlargement.ec.europa.eu/system/files/2018-12/20161109_report_bosnia_and_herzegovina.pdf

[6] http://www.revizija.gov.ba/Post/Read/izvjestaj-revizije-ucinka-aktivnosti-institucija-bih-na-osiguranju-osnovnih-pretpostavki?lang=sr

[7] https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-ENG-WEB.pdf

[8] https://fena.ba/article/1299130/u-bih-nedostaje-strateski-i-zakonski-okvir-kibersigurnosti

[9] https://www.undp.org/bs/bosnia-herzegovina/news/poceo-13-miliona-eura-vrijedan-projekat-za-izgradnju-cyber-sigurnosti-u-bosni-i-hercegovini

[10] https://www.portalanalitika.me/clanak/nato-donira-bih-sisteme-za-sajber-bezbjednost

[11] https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[12] https://detektor.ba/wp-content/uploads/2022/12/Cyber-sigurnost-FINAL-WEB-pages-1.pdf

[13] https://www.nato.int/cps/en/natohq/official_texts_133177.htm

[14] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[15] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity

[16] https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

[17] https://balkaninsight.com/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/

[18] https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-ENG-WEB.pdf

[19] https://fena.ba/article/1299130/u-bih-nedostaje-strateski-i-zakonski-okvir-kibersigurnosti

[20] http://www.sluzbenilist.ba/page/akt/g4E0HNrVpsc=

[21] https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/Bosnia%20and%20Herzegovina%20Report%202022.pdf

[22] https://www.vijeceministara.gov.ba/saopstenja/sjednice/saopstenja_sa_sjednica/default.aspx?id=40377&langTag=bs-BA

[23] https://detektor.ba/wp-content/uploads/2022/12/Cyber-sigurnost-FINAL-WEB-pages-1.pdf

[24] https://istinomjer.ba/i-bih-ima-regulativu-iz-oblasti-kiberneticke-bezbjednosti/

[25] https://balkans.aljazeera.net/teme/2023/1/29/kako-bih-moze-povecati-otpornost-na-cyber-napade

[26] https://fbihvlada.gov.ba/bs/utvrden-nacrt-zakona-o-informacionoj-sigurnosti-fbih

[27] https://izis.org/wp-content/uploads/2020/09/IZIS_080UPP_110ZAK_Zakon_o_informacionoj_bezbjednosti.pdf

[28] https://business-magazine.ba/2022/09/06/cyber-kriminal-bih-se-povecava/

[29] https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-ENG-WEB.pdf

[30] http://www.revizija.gov.ba/Post/Read/izvjestaj-revizije-ucinka-aktivnosti-institucija-bih-na-osiguranju-osnovnih-pretpostavki?lang=sr

[31] https://balkaninsight.com/2022/09/12/western-balkans-urged-to-prepare-for-uptick-in-cyber-attacks/

[32] https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/upozorenje-iz-nato-a-rusija-bi-mogla-izvesti-velike-cyber-napade-u-bih/457254

[33] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658404

[34] https://www.osce.org/files/f/documents/1/a/438383.pdf

[35] https://www.pwc.rs/en/publications/cybersecurity-ecosystem-report.html

[36] https://www.undp.org/bs/bosnia-herzegovina/news/poceo-13-miliona-eura-vrijedan-projekat-za-izgradnju-cyber-sigurnosti-u-bosni-i-hercegovini

[37] https://www.pwc.rs/en/publications/cybersecurity-ecosystem-report.html

[38] https://en.imsilkroad.com/p/118790.html

[39] https://www.nato.int/cps/en/natohq/news_210741.htm

[40] https://www.slobodnaevropa.org/a/bih-nato-cyber-bezbjednost/32283447.html

[41] https://mup.vladars.net/lat/index.php?vijest=13826&vrsta=saopstenja

[42] https://www.vladars.net/eng/vlada/ministries/MST/infocent/News/Pages/MoUIsraelELTA.aspx

[43] https://vecernjenovosti.ba/120273/vijesti/sajber-akademija-u-srpskoj-vlada-rs-potpisala-ugovor-sa-izraelskom-kompanijom/

[44] https://www.pwc.rs/en/publications/cybersecurity-ecosystem-report.html

[45] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658404