Regional Report:

Cyberattacks and Digital Identity in the Balkans

Greater Internet Freedom

Balkan Investigative Reporting Network (BIRN)

June 2023

Table of Contents

Acknowledgements

The following BIRN* team members contributed to this report:

a. **Journalists/Researchers:** Gjergj Erebara, Azem Kurtic, Xheneta Murtezaj, Bojan Stojkovski, Igor Ispanovic

b. **Editor:** Ivana Jeremic

c. **Fact-checking:** Milica Stojanovic

d. **Expert opinion:** Predrag Tasevski

e. **Digital Rights Programme Manager:** Miloš Ćirić

f. **Project Manager:** Amina Mahović

g. **Digital Rights Researcher:** Matteo Mastracci

**BIRN is a network of non-governmental organizations promoting freedom of speech, human rights, and democratic values in Southeast and Eastern Europe. BIRN strives to empower people to access their rights by providing accurate and relevant information and creating opportunities for them to participate in democratic processes. Through high-quality reporting and by creating a pool of skilled journalists, BIRN examines and scrutinizes key processes, steers debates and provides the public with impartial and reliable information.*

This report is published under the USAID Greater Internet Freedom (GIF) project implemented by Internews and the GIF consortium.

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the Balkan Investigative Reporting Network and do not necessarily reflect the views of USAID or the United States Government.

Executive Summary

This report focuses on the following Balkan countries: Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, and Serbia, and is part of a multi-region research aimed to identify and compare the state of biometrics and digital identity threats, usage, and impact in Africa, the Balkans, Central Asia, Latin America and the Caribbean, and South and Southeast Asia.

The report delves into cybersecurity threats, namely exploits, phishing, malware, and ransomware, and vulnerabilities faced by five countries in the Balkan region (also Balkan or Balkans) for the period 2020-2023. The focus countries include Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, and Serbia. This research is centered on an investigation and analysis of data collated into a database detailing notable cyber-attacks on critical infrastructure and public institutions' servers and revealing large data breaches and leaks, with implications for entities' digital identity protection in the region.

As the analysis unfolded, key regional trends emerged, such as the growing reliance on biometrics and digital identity (BDI) for online banking, e-government services, and border control. This reliance was primarily driven by advancements in technology, which aimed to enhance security, streamline processes, and ensure more efficient and reliable authentication methods. However, the implementation of BDI systems has raised concerns about the safeguarding of individuals' right to privacy and data protection, and the potential misuse of personal information.

The researchers investigating these prominent cyber incidents employed a mixed-methods approach, utilizing qualitative content analysis as their primary method. This involved systematically analyzing and interpreting data from diverse sources, including government reports, news articles, and information obtained through requests made to the authorities. The combination of qualitative content analysis and data triangulation allowed for a

comprehensive examination of the cyber incidents, enhancing the depth and accuracy of the research findings.

Key Findings

The report identifies key challenges in addressing cybersecurity threats in the Balkan region, including the need for increased public awareness, inadequate cybersecurity policies and practices, and limited regional collaboration in combating cybercrime. The research emphasizes that the Balkan region faces significant risks as well as opportunities due to its increasing reliance on BDI. The key findings include:

- A significant surge in cyberattacks, particularly phishing and ransomware, was observed in all five Balkan countries between 2020-2023.
- The public sector, banks, and individual citizens were among the most frequently targeted entities.
- Perpetrators were able to exploit vulnerabilities in the digital infrastructure and security measures of both private and public entities.

Key Recommendations

To tackle these challenges, the report proposes recommendations for governments, organizations, and individuals, including public awareness campaigns, investment in comprehensive cybersecurity policies and practices, greater regional collaboration, and more. These are centered around safeguarding privacy, security, and trust in online transactions and interactions. By implementing these recommendations, governments, organizations, and individuals can collectively respond to the evolving cyber landscape and proactively protect their digital environments.

- Enhancing cybersecurity measures across public and private sectors.
- Increasing public awareness and education on phishing and other cyber threats.
- Enhancing regional cooperation and information sharing among the countries researched.

Introduction

The digital realm has become an integral part of our lives, with digital identity representing individuals, organizations, and entities online, while biometrics are used for identification and authentication purposes. Digital identity encompasses online information, credentials, and attributes such as usernames, passwords, biometric data, and personal details. Biometrics are unique biological, behavioral, and physiological characteristics, such as fingerprints, facial features, voice patterns, and iris scans. Biometrics and digital identity (BDI) play a vital role in preserving privacy, security, and trust in online transactions and interactions.

Between 2020 and 2023, the Balkan region experienced a significant internet penetration increase, ranging from 75% to 96%. This was accompanied by technological advancements, such as the integration of BDI technology into public and private systems and services, underscoring the need for robust cybersecurity measures. For instance, BDI has been seamlessly incorporated into various digital platforms serving diverse purposes, such as online banking for financial transactions, digital government services for border control and law enforcement, e-commerce websites for online commercial transactions, mobile applications for integration into user's digital devices, amongst others.

This report investigates the nature, extent, and impact of cyberattacks in five Balkan countries between 2020 – 2023, noting that the rising adoption of BDI technologies in the Balkan region has opened new avenues for cybercriminals to exploit. In particular, the research examines the prevailing cybersecurity threats, government and stakeholder responses, and broader regional trends and developments. The study aims to raise awareness about cybersecurity challenges in the Balkans, offers insights into the factors driving vulnerabilities and threats in BDI systems, and suggests the strengthening of cybersecurity measures across both public and private sector.

The report findings reveal the existence of cybersecurity vulnerabilities in BDI systems and networks, which have been exploited, as evidenced by the escalating frequency of cyberattacks targeting online infrastructure, servers, e-services, websites, and computers. Further, the report finds that the Balkan countries examined in this report faced numerous cybersecurity threats, intensified by inadequate public awareness, insufficient cybersecurity policies, and a lack of regional collaboration in addressing cybercrime.

These cybersecurity vulnerabilities and threats have compromised the security and integrity of BDI systems, affecting their overall reliability. Moreover, only a few countries in the region have implemented or are currently implementing data protection laws and regulations aligned with the European Union's General Data Protection Regulation (GDPR). For instance, Croatia, Serbia, Montenegro, Albania, and North Macedonia have taken steps to align their data protection laws with the EU GDPR. However, the enforcement of these laws and overall awareness about data protection and privacy remain inconsistent across the region.

- Croatia implemented the Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) in 2018, which provides rights and obligations similar to the GDPR.
- Serbia adopted the Law on Personal Data Protection (*Zakon o zaštiti podataka o ličnosti*) in 2018, aligning with the principles and requirements of the GDPR.
- Montenegro enacted the Law on Personal Data Protection (*Zakon o zaštiti podataka o ličnosti*) in 2019, bringing its data protection laws in line with the GDPR.
- Albania has made progress towards aligning its legislation with the GDPR and adopted the Law on Personal Data Protection in 2020 to achieve European standards.
- North Macedonia is in the process of aligning its data protection laws and has taken a significant step by adopting the Draft Law on Personal Data Protection in 2021, aiming to harmonize its regulations with EU standards.

By exploring specific challenges and threats faced by each country and broader regional trends, this research seeks to identify the key factors shaping the cybersecurity landscape and propose actionable recommendations for mitigating cyber threats and vulnerabilities.

Methodology

Table 1: Research Topic and Research Questions (by BIRN)

Research Topic	Cyberattacks and Digital Identity in the Balkans
Research Questions	❖ What are the specific cybersecurity vulnerabilities present in biometrics and digital identity (BDI) systems and networks in the five Balkan countries under study? ❖ What are the prevailing cybersecurity threats faced by the Balkan countries in the specified timeframe (2020-2023)? ❖ What are the broader regional trends and developments in cybersecurity in the Balkans during the specified timeframe? ❖ What insights can be gained from this research to enhance the overall cybersecurity measures in the Balkan region?

To explore the intricate world of BDI and cybersecurity in the Balkan region, this research adopted a qualitative approach using mixed methods, including a desk review of relevant studies and reports, interviews with IT employees at IT departments in public companies and institutions, and the case study research design. This research methodology is appropriate for enabling a deep understanding of the complex relationship between cybersecurity and BDI in the Balkan region. This region was selected because of its technological advancements and a wave of cyberattacks affecting Balkan economies.

A multifaceted data collection approach was employed for this research, including document analysis and case study examination. The researchers first conducted a literature review of government and NGO reports, news articles, and industry reports. These painted a vivid picture of the current state of BDI in the Balkan region, shed light on associated cybersecurity threats, and lay a solid foundation for understanding the study's broader theoretical and empirical context. Secondly, the researchers collated data on notable cyberattacks targeting the Balkan region's BDI systems into a database and conducted interviews with IT employees. Selected case studies offered invaluable insights into cyberattacks on critical infrastructure and public institutions' servers and revealed large data breaches and leaks.

To analyze the data, the report relied on qualitative content and comparative analysis methods to analyze cyberattack incidents across five Balkan countries. The research also relied on triangulation, a technique used in mixed-methods research, to enhance validity and reliability by cross-checking data from different sources. These data analysis methods and techniques were appropriate for this research and (i) enabled the identification of patterns and themes emerging from the collected data allowing a systematic and structured analysis, (ii) facilitated triangulated comparisons across data sources and countries ensuring the robustness and credibility of research findings, and (iii) assisted with the identification of similarities and differences in cybersecurity and BDI landscapes across the Balkan region. The research also benefited from an external expert review written by Predrag Tasevski and was improved based on comments he provided.

As a result, the research was able to address the research questions, identify regional trends, assess the effectiveness of different policy and practice approaches, and inform recommendations for, amongst others, regional collaboration, and knowledge sharing.

Research Limitations

This research report was limited by the following:

- ***Data availability and limitations:*** The research relied heavily on secondary data sources, whose availability and reliability varies. In addition, available data might not provide a complete picture of the cybersecurity vulnerabilities, incidents, and responses in the Balkan region. Critical incidents or relevant data may have been missed or have not been accessed, potentially affecting the accuracy and comprehensiveness of the research findings.
- ***Interpretation biases:*** The analysis and interpretation of data are subject to the researchers' biases and subjectivity.
- ***Timeframe of the research:*** The researchers restricted the report timeframe between 2020 to 2023. Emerging trends and developments beyond this timeframe have not been captured in this research.

Operational Terms

Biometrics	Set of unique physical or behavioral characteristics, including fingerprints, facial or voice recognition, amongst others, used to identify and authenticate individuals. Increasingly, biometric technology is being used for other functional purposes including border control, election management, financial transactions, refugee management, health.
Cyber attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Cyber espionage	A type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage, or political reasons.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
Cyber threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Cybersecurity vulnerabilities	Any weakness within an organization's information systems, internal controls, or system processes that can be exploited by cybercriminals.
Digital identity	Data that uniquely describes a person, organization or other entity in the digital world.
Distributed denial-of-service (DDoS)	A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Exploit-based attacks	Types of cyberattacks that take advantage of vulnerabilities or weaknesses in computer systems, networks, or software to gain unauthorized access or control. Attackers use specialized code or techniques, called exploits, to exploit these vulnerabilities and compromise the targeted system. These attacks can lead to data breaches, unauthorized access, or the installation of malware. Regular software updates and strong security measures are crucial to prevent such attacks.
Insider threat	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Personal information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Phishing attacks	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.
Ransomware	A type of malicious software that encrypts a user's data and demands a ransom payment for its release, often targeting individuals, businesses, or public institutions.
Sensitive information	Data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or social security numbers.

Results/Analysis: Cyber Attacks and Digital ID in the Balkans

Comparative Analysis

The research unveils numerous challenges related to cybersecurity threats/vulnerabilities and digital identity across the five researched countries (Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, and Serbia) between 2020-2023. Key challenges and threats that the research unveiled include cyberattacks, phishing attacks, lack of cybersecurity awareness and education, limited resources, and capabilities (such as funding, specialized personnel, and training programs), and inadequate legal and regulatory frameworks. However, despite many commonalities, each country experiences unique incidents and issues that are addressed individually in the case studies below.

The goal of this comparative analysis is to search for similarity and variance among units of analysis. By carrying out a comparative analysis relying on an incident database tracker, the following trends from the five Balkan countries were revealed:

- All five countries have experienced cyberattacks on their BDI systems, with phishing attacks (10) being the most prevalent. Ransomware attacks also ranked high in frequency (9), followed by exploit-based attacks (8). There were three instances of unknown attacks, as well as isolated cases of malware and DDoS attacks (one time each). These findings emphasize the need for stronger cybersecurity measures and infrastructure protection.
- Phishing attacks are prevalent in each country, with cybercriminals targeting individuals and organizations to obtain sensitive personal information with an impact on individuals' right to privacy and data protection. This underscores the importance of raising cybersecurity awareness and education among the general population and organizations.
- Insider threats or employee negligence pose significant risks in all countries, originating from individuals within an organization who have access to sensitive information and systems and either advertently or inadvertently fail to safeguard

this data. This emphasizes the need for strict access controls, ongoing education, training, and monitoring, and stringently enforced security protocols and policies.

- All countries face challenges related to limited resources and capabilities when addressing cybersecurity threats and challenges. Budget constraints, lack of skilled cybersecurity professionals, and insufficient investment in technology and infrastructure can hinder the development and implementation of robust security measures.
- Enforcement of existing laws and regulations in rapidly evolving digital landscapes is proving difficult, especially with outdated or unenforceable laws. This revealed the need to support law enforcement agencies and regulators with additional resources, capacity-building support, and clear jurisdictional frameworks for pursuing and prosecuting cybercriminals effectively.
- International cooperation and information sharing are crucial for protecting BDI systems in all five countries. The promotion of effective information sharing and fostering stakeholder collaboration is necessary to achieve this goal. We propose that governments in five Balkan countries strengthen engagements with international initiatives such as:
    - Global Cybersecurity Alliance (GCA),
    - Cybersecurity and Infrastructure Security Agency (CISA),
    - Cybersecurity Tech Accord,
    - Forum of Incident Response and Security Teams (FIRST), and
    - Global Forum on Cyber Expertise (GFCE).

Addressing cybersecurity challenges impacting BDI systems in the Balkan region requires a multifaceted approach. This should be grounded in enhancements to legal and regulatory frameworks, improvements in cybersecurity awareness and education, strengthened critical infrastructure protection, and a promotion of international cooperation and information sharing. These efforts will help build a more resilient and secure environment for BDI systems across the region.

Country Case Studies

Albania

In July 2022, Albania's digital ID system suffered a cyberattack that compromised the biometric data of 910,000 citizens, raising concerns about the effectiveness of security measures and sensitive personal information protection. A massive database of 910,000 voters in the Tirana region that contained personal data, such as IDs, job titles and even possible political preferences, was published by the media. The investigation into this breach revealed that an organized criminal group exploited vulnerabilities in the system's software and infrastructure, which were caused by inadequate security measures, ineffective system maintenance, inadequate monitoring, and a failure to properly integrate data protection and privacy principles into BDI systems.

In addition to biometric identity data breaches, phishing attacks have been prevalent in Albania, with cybercriminals targeting individuals and organizations to obtain sensitive personal information. One notable case occurred in April 2021 when a phishing campaign focused on clients of an Albanian bank, using fake emails that appeared to come from the bank's official domain to harvest login credentials and other sensitive data.

The country also faces significant concerns related to cyberattacks on critical infrastructure, such as energy and telecommunications systems. BDI systems rely on the availability, security, and functionality of critical infrastructure, such as power supply, to function optimally. Illustratively, in September 2021, an attack on Albania's power distribution network led to widespread outages that impacted use and access of BDI systems, highlighting the urgent need for stronger cybersecurity measures to protect critical infrastructure.

Insider threats pose another significant risk to BDI in Albania, originating from individuals within an organization who have access to sensitive information and systems. In a striking example, an employee of an Albanian government agency was arrested for selling citizens' personal identification numbers and other sensitive data on the dark web.

Government agencies worldwide, including Albanian government agencies, frequently face challenges related to limited resources and capabilities when addressing cybersecurity threats. Budget constraints, a lack of skilled cybersecurity professionals, and insufficient investment in technology and infrastructure can all hinder the development and implementation of robust security measures to protect BDI systems.

Albania's cybersecurity landscape highlights significant threats and challenges related to BDI. Addressing these issues requires a comprehensive and coordinated approach involving:

- Robust security measure development and implementation,
- Investments in technology and infrastructure,
- Cybersecurity awareness and education improvements, and
- Establishing a clear and effective legal and regulatory framework for data protection and privacy.

Bosnia and Herzegovina

In Bosnia and Herzegovina (BiH or B&H), the cybersecurity landscape is also marked by various challenges that pose significant threats to BDI. Data breaches are a prominent issue resulting from weak security measures, software vulnerabilities, and targeted cyberattacks.

BiH provides its citizens with biometric documents, including IDs and passports. Considering the complicated country structure with divided power sharing and responsibility, most of the country still does not use electronic health insurance cards. The health sector is digital in only three out of ten cantons (i.e., a governance tier focused on administrative local government) in the Federation of Bosnia and Herzegovina entity, and on the whole territory of *Republika Srpska*, Bosnia’s other administrative unit. BiH is ‘comprised of four tiers of governance, at the State, Entity, Canton, and municipal levels.

Phishing attacks are widespread in BiH, with cybercriminals deceiving individuals and organizations into revealing sensitive information such as email addresses and other personally identifiable information (PII). In October 2022, the Federation entity police warned citizens about phishing campaigns aimed at citizens. The phishing emails sought to deceive recipients into disclosing sensitive information, including their email addresses and other PII. Similarly, in April 2023, a phishing campaign involving fraudulent emails was discovered, where fraudster impersonating Mirsad Vilić, the Director for the Directorate for

Coordination of Police Bodies B&H, using police and Europol logos, targeted a significant number of citizens, particularly directors and managers of companies. Further, a phishing campaign in 2020 targeted clients of a bank, using the bank's brand identity. Bank warned its clients not to provide any personal data via email, Facebook, or Viber, citing complaints of misuse of clients' personal data. Similar warnings were issued in 2021, indicating that cyberattacks may have been flagged.

These incidents underscore the importance of raising customers' and users' cyber safety awareness and implementing robust security measures. For users, education on phishing risks in the country is critical, whereas public and private sector entities should deploy technical safeguards such as email authentication, web filtering, anti-phishing software, training, intrusion detection, browser protections, security management, endpoint protection, network segmentation, and regular audits.

The country's evolving legal and regulatory cybersecurity and digital identity protection framework has gaps and inconsistencies. While progress has been made in adopting new legislation in recent years, introducing amendments on computer fraud and crimes into criminal codes of the cantons, entities, and state-level criminal codes, challenges remain in harmonizing existing laws across all levels of the Bosnian government.

Capacity-building efforts are needed in law enforcement and regulatory agencies, starting with awareness raising. BiH finds itself in a disadvantaged position, being the last Western Balkans country with no functioning all-encompassing Computer Security Incident Response Team (CSIRT). This leaves BiH, its government, economy and citizens exposed to cyber harm that may jeopardize the potential benefits of digitalization for the economy and society, and the country more vulnerable to malign external influences in the cyber domain. To mitigate this risk, in 2020, the Cyber Security Excellence Centre (CSEC) was established, as part of the Criminal Policy Research Centre, to strengthen cybersecurity in BiH. The Government of the United Kingdom provided financial and expertise support.

Addressing cybersecurity challenges in Bosnia and Herzegovina requires a multifaceted approach that includes:

- Enhancing the legal and regulatory framework,

- Improving cybersecurity awareness and education,
- Strengthening critical infrastructure protection, and
- Promoting international cooperation and information sharing.

Kosovo

Kosovo is modernizing its digital infrastructure through the formulation of the Digital Agenda 2030. Kosovo has implemented BDI systems to enhance public services, foster economic development, and promote social inclusion, with the launch of various initiatives like biometric passports. The Kosovo biometric passport has been issued since October 31, 2011, and the country has expanded its e-government services as part of a broader digital strategy to become a prosperous digital nation. Illustratively, Kosovo developed a state portal "E-Kosova" offering public services electronically. The country is exploring biometric technologies for law enforcement and border management.

As a demonstration of its political will and commitment towards digitalization, Kosovo joined the EU Digital Agenda for Western Balkans in 2018. In 2022 a Kosovo Digital Agenda 2030 was drafted, and the Strategy for Public Administration Reform (2022-2027) was developed to support national development.

In the last three years, Kosovo experienced a wave of cyberattacks that impacted various industries. Illustratively, a cyberattack was launched against Kosovo Telecom in September 2022, with government services also being attacked, leading to internet service disruptions and the inaccessibility of several government websites. In April 2020, one of the largest banks operating in Kosovo, *Banka Ekonomike*, was attacked with the DoppelPaymer ransomware. According to one Danish Center for Cyber Security threat assessment, the hackers leaked more than 70 GB of customers' financial transactions data, including client names, credit card numbers, income, and loans. Sensitive information belonging to bank employees was also leaked.

In response to these challenges, Kosovo adopted the Strategy and Action Plan for Cyber Security (2016-2019) to ensure a safe cyber space environment, minimizing and preventing cyber threats in cooperation with local and international partners. The government also established a National Computer Incident Response Team (KOS-CERT) and enhanced its legal and regulatory framework for cybersecurity and digital identity protection.

In 2020, the Government of Kosovo prepared the new draft Law on Cyber Security, which entered into force in February 2023, and provides for the prevention of cybercrime relying on criminal offenses. The law is also expected to strengthen law enforcement capacity, which is currently limited, through the establishment of the State Authority for Cyber Security. The law also proposes to establish a contact point in The Kosovo Police, which will be accessible 24 hours, 7 days a week.

Despite these efforts, Kosovo still faces significant challenges in ensuring the security and privacy of its BDI systems. The need for comprehensive legislation, the limited capacity of law enforcement, and the lack of public awareness continue to undermine the government's efforts to enhance cybersecurity. These challenges were reiterated in the Progress Report of the European Commission for Kosovo in 2022.

According to the report, in 2021, there were 37 reported cases of cybercrime in Kosovo, a decrease from the previous year's 53 cases. Despite these cases, there were no indictments or final judgments made, and one investigation was terminated. The Kosovo Police Sector for the Investigation of Cybercrime initiated four cases related to the offense of Child Abuse in Pornography, and three criminal charges were filed against 17 individuals.

Kosovo needs a comprehensive and coordinated approach to address cybersecurity concerns and protect its BDI systems by:

- Addressing cybersecurity issues within government institutions and agencies, including
    - ❖ hiring qualified cybersecurity professionals' and engaging in capacity-building through professional development programs
    - ❖ providing cybercrime training for newly appointed judges and prosecutors and individuals responsible for handling electronic evidence to equip them with the necessary expertise to effectively investigate and prosecute cybercrimes

    - enhancing the capacity of law enforcement and regulatory authorities through targeted training programs, technical assistance, and resource allocation.
- Strengthening the legal and regulatory framework by ensuring the effective enforcement of cybersecurity and data protection laws, including the Law on Prevention and Fight of the Cyber Crime and the Law on Protection of Personal Data.
- Implementing public awareness campaigns through the KOS-CERT to educate citizens and organizations about cybersecurity risks and best practices, including
    - engaging academia and civil society groups to provide extracurricular programs to civilians and students
    - creating and disseminating educational material online and offline informing citizens about potential and actual cyber security threats.
- Promoting international cooperation and information sharing with international partners.
- Encouraging innovative cybersecurity solutions and local industry growth by supporting research, fostering public-private partnerships, and creating an enabling environment for cybersecurity startups.

North Macedonia

North Macedonia is experiencing rapid digitalization, leading to a growing reliance on BDI to deliver public and private services. While this transition enhances efficiency in service delivery and transparency, it also exposes the country to various cybersecurity threats that can affect digital infrastructure, citizen privacy, and national security.

When it comes to digital identity, a partnership between Mastercard and the country's Ministry of Information Society and Administration brought local digital identity and related services, such as digital document signing and verification, to Macedonian citizens in late 2021. However, these services are not widely used in the country.

Between 2020 to 2023, the country has faced numerous cyberattacks and threats, broadly categorized into three main types: distributed denial-of-service (DDoS) attacks, phishing campaigns, and cyber espionage. DDoS attacks often target public institutions, causing disruption and downtime. Phishing campaigns aim to deceive individuals into revealing sensitive information, while cyber-espionage operations infiltrate and exfiltrate sensitive data from government and private sector organizations.

In response to these threats, North Macedonia adopted the National Cybersecurity Strategy, outlining strategic goals for enhancing cybersecurity, such as improving critical infrastructure protection and fostering international cooperation. The government established the National Center for Computer Incident Response (MKD-CIRT) to implement the strategy and introduced legislation, such as the Law on Security of Networks and Information Systems (2019), to support cybersecurity efforts.

Despite these efforts, North Macedonia faces challenges and vulnerabilities, such as lacking adequate technical expertise and resources, low cybersecurity awareness among citizens and organizations, and a fragmented cybersecurity landscape. Therefore, the cyberattacks that organizations and citizens have experienced during the past few years should serve as a warning to authorities and add to the urgency of being better prepared when it comes to dealing with similar potential cases in the future.

While the country has made progress in developing its cybersecurity framework and initiatives, it must continue building on these foundations. By investing in capacity building, enhancing cybersecurity awareness, strengthening public-private partnerships, and promoting international cooperation, North Macedonia can better protect its digital infrastructure, safeguard citizen privacy, and ensure national security. We urge the government to protect its systems by:

- Investing in capacity building by developing domestic cybersecurity expertise.
- Enhancing cybersecurity awareness through intensified public awareness campaigns by the MKD-CIRT and other stakeholders.
- Strengthening public-private partnerships to leverage resources and expertise in addressing cybersecurity challenges through:
    - ❖ Sharing resources, expertise, and technologies to enhance cybersecurity capabilities. Specifically, leverage public sector's funding and regulatory capabilities and private sector's technological expertise and innovation.
    - ❖ Joint facilitation of research/development efforts.
    - ❖ Forming cybersecurity information exchanges.

- Establishing internal, formal, channels/platforms for sharing threat intelligence/best practices/lessons learned for law enforcement agencies.
- Promoting international cooperation by engaging in international cybersecurity forums and partnerships. Specifically, authorities and other cybersecurity stakeholders should consider attending regional and international cybersecurity forums where they could learn from the experience of countries that have dealt with similar cyberattacks and learn about best practices.

Serbia

Serbia has experienced rapid digitalization and increased information and communication technologies (ICTs) use in recent years. The number of mobile phones and computers per household has been rather high and is steadily increasing on an annual basis. According to the latest report by the Statistical Office of the Republic of Serbia, 95% of households own a mobile phone, while 77% have a computer. However, the COVID-19 pandemic accelerated the digital transformation and the uses of technologies in specific sectors, such as education, banking, government services and e-commerce. For example, more than 30% of cardholders in Serbia started using mobile payments during COVID-19.

On the other hand, the application of BDI posed concerns when the Serbian government proposed the draft of the new Law on Internal Affairs, which would enable the use of mass surveillance technologies developed by Huawei. The draft was withdrawn twice, most recently in late December 2022.

Serbia has made significant progress in developing its cybersecurity infrastructure and policy framework. The country adopted the Law on Information Security in 2016, which marked the first time this sector was regulated. The Law set out to establish the measures for the protection against security risks in information and communication systems, the responsibilities of legal entities in managing and using these systems and coordinate the monitoring and communication between relevant actors. The amendments to the Law on Information Security, adopted in October 2019, brought this area closer to the legal framework of the European Union, i.e., the Network and Information Security (NIS) Directive.

Moreover, the National Security Strategy adopted in 2021 identified cyber threats and their prevention as an important component in preserving national security. It recognized that the safety of cyberspace will primarily be in danger of espionage, attacks on critical infrastructure, unauthorized intrusion into classified databases and spreading fake news and misinformation via social networks.

The government has also established the National Computer Emergency Response Team (CERT) and a national cybersecurity center. Despite these advancements, Serbia needs more resources and capacity to effectively address cyber threats, including limited funding, specialized personnel, and training programs. According to the current Strategy on Development of Information Society and Information Security, only one fifth of companies in the country have employed cyber security experts, while more than three quarters hire externally. Additionally, only one quarter organize training on digital skills for all their employees.

Furthermore, many Serbian citizens, businesses, and organizations need to gain basic cybersecurity knowledge. Employees at IT departments in public companies and institutions stressed out that staff often use their business computers and accounts for private purposes and have issues recognizing scam and phishing emails.[1]

Overall, this growth has led to a rise in cyber threats, making cybersecurity a critical concern. Several high-profile cyber incidents highlight Serbia's cybersecurity vulnerabilities. On March 1, 2020, public utility company "*Informatika*'' in Novi Sad, a city in Serbia, was attacked with malware Pw ndLocker. Due to the incident, the servers of city administrations and other public services did not work the following day, as well as the city cameras, while the staff at the company could not access their emails. The perpetrators asked for a ransom, which the city refused to pay.

Another major incident occurred two years later, when the infrastructure of the Republic Geodetic Authority was compromised. The attackers blocked its database for nine days and the system was only reinstated fully after three weeks. In both cases, officials claimed that citizens' data was not jeopardized.

[1] Interviews with employees at IT departments in public companies and institutions (May 24 and May 31, 2023).

Other notable cases include multiple phishing campaigns targeting the Serbian Post Office, financial institutions, and the National Bank of Serbia, where perpetrators used various methods to obtain citizens' financial data or impersonate institutions and their services. For example, perpetrators pretending to be the Serbian Post Office sent emails as alleged reminders to recipients that the Customs Office held up their packages because a certain fee was not paid. The link in these messages led to a fake domain, which required citizens to fill in their financial data. A similar tactic is sometimes utilized via SMS and other messaging apps.

Serbia's cybersecurity landscape requires a comprehensive and coordinated approach to address its challenges and threats. Serbia has made strides in developing its cybersecurity infrastructure and policy framework, but more work is needed to ensure resilience. The Serbian government is urged to address complex cybersecurity concerns and protect its BDI systems by:

- Fostering public-private partnerships and strengthening the Cyber Security Nexus (formally the "Petnica group"), a PPP established in 2015 between the Organization for Security and Co-operatation in Europe Mission to Serbia, Diplo Foundation, the Geneva Centre for Security Sector Governance, and the Petnica Research Center, by:
    - ❖ Producing additional guides, similar to the 'Guide through Information Security' in the Republic of Serbia, for Serbian stakeholders.
- Contributing to regional cooperation through Serbia's continued membership and participation in:
    - ❖ United Nations Open-Ended Working Group on Cyber and Information Security.
    - ❖ Global Forum on Cyber Expertise,
    - ❖ OSCEs informal working group on cyber security.
- Implementing the National Security Strategy and improving the general security culture of all citizens and raising the skills and capacities for processing, transferring and protection of information-communication systems.

Conclusion and Recommendations

The study of cybersecurity threats and vulnerabilities exacerbated by cyberattacks in Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, and Serbia reveals several trends and shared problems that call for immediate attention and a coordinated regional response. This conclusion highlights the main findings of this research, identifies the common issues faced by the countries in the Balkan region and suggests potential solutions to strengthen their cybersecurity posture.

Trends and Shared Problems

- Phishing attacks are prevalent in all five countries, with cybercriminals targeting both individuals and organizations, particularly financial institutions. The attackers often pose as representatives of legitimate entities, such as banks or government institutions, to trick victims into revealing their sensitive information or downloading malicious software.
- Ransomware attacks have been on the rise in the region, with hackers using increasingly sophisticated methods to target businesses, public institutions, and individuals. These attacks not only cause significant financial losses but also disrupt critical services and infrastructure.
- The lack of sufficient investment in cybersecurity measures and the absence of comprehensive legal and regulatory frameworks in some countries exacerbates cybersecurity challenges for the whole region. This leads to inadequate protection of critical infrastructure, businesses, and citizens from cyber threats.

Recommendations

The Balkan region faces various cybersecurity challenges that require a concerted and coordinated response from governments, businesses, and individuals. By implementing the recommendations outlined below, the countries in the region can strengthen their resilience to cyberattacks and threats, protect their critical infrastructure and citizens, and contribute to a more secure and stable digital environment.

To address these risks, the report proposes the following recommendations to the governments, businesses, and individuals in the Balkan region:

Enhance Regional Cooperation on Cybersecurity

- Given the transnational nature of cyberthreats, regional cooperation is crucial for effectively addressing cybersecurity challenges. The Balkan countries should collaborate more closely on sharing threat intelligence, best practices, and resources to develop a unified and coordinated response to cyber threats.

Strengthen Legal and Regulatory Frameworks

- Governments should review and/or update their legal and regulatory frameworks to address emerging cyber threats effectively.

Invest in Cybersecurity Infrastructure and Capacity Building

- Both public and private sectors need to invest in improving their cybersecurity infrastructure, including the deployment of advanced security technologies and the development of skilled cybersecurity professionals. This can be achieved through increased public funding, public-private partnerships, and collaboration with international organizations and experts.

Raise Awareness and Promote a Culture of Cybersecurity

- The general public must be informed of the risks associated with cyber threats and the steps they can take to protect themselves. Governments, businesses, and civil society should work together to develop and implement awareness campaigns, educational programs, and training initiatives to promote a culture of cybersecurity in the region.

Develop and Implement National and Sector-Specific Cybersecurity Strategies

- Each country in the region should develop and implement a comprehensive national cybersecurity strategy that addresses the specific risks and vulnerabilities faced by the country. Additionally, sector-specific strategies should be developed for critical infrastructure and industries that rely on biometrics and digital identity, such as finance, energy, and telecommunications.

Foster Innovation and Research in Cybersecurity

- Governments and businesses should support research and innovation in cybersecurity by providing funding, resources, and opportunities for collaboration. This can help develop cutting-edge solutions to emerging cyber threats and contribute to the overall resilience of the region.

Engage with International Partners and Organizations

- The Balkan countries should actively engage with international partners, such as the EU, NATO, and the UN, and individual countries that support cybersecurity efforts, to access additional resources, expertise, and support in addressing cybersecurity challenges.

Prioritize the Protection of Digital Identity and Biometrics

- As more services and transactions move online, securing digital identity and biometric data becomes increasingly critical. Balkan governments should establish robust data protection frameworks and ensure that adequate safeguards are in place to protect the privacy and security of citizens' digital identity and biometric information.

Reference List

Council of Europe, Convention on Cybercrime (Budapest Convention), 2021.

Drobnič S, Comparative Analysis. In: Michalos, A.C. (eds) Encyclopedia of Quality of Life and Well-Being Research. Springer, Dordrecht, 2014.

EKosova, Platforma e shërbimeve online.

European Commission - Commission Staff Working Document, Kosovo 2022 Report SWD 334, (2022).

European Committee of the Regions (CoR), Bosnia-Herzegovina.

European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

European Union Agency for Cybersecurity (ENISA), Threat Landscape for Telecommunications Infrastructure, 2020.

Geneva Centre for Security Sector Governance, National Cybersecurity Strategies in Western Balkan Economies, 2021.

International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2020.

Interpol, Cybercrime, 2020.

Kshetri, N., Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Journal of Balkan and Near Eastern Studies, 2016.

NATO, Cyber Defence, 2021.

Organization for Security and Co-operation in Europe (OSCE), Cyber/ICT Security, 2020.

Pravno Informacioni Sistem, 2021.

Republika e Kosovës, Agjenda Digjitale e Kosovës 2030, 2023.

Republika e Kosovës, Law No. 06/L-082 on the Protection of Personal Data, 2019.

Republika e Kosovës, LIGJI NR. 03/L-166 Për Parandalimin dhe Luftimin e Krimit Kibernetikë, 2010.

Republika e Kosovës, Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit, 2016 – 2019.

Republika e Kosovës, Ligj Për Sigurinë Kibernetike, 2023.

Share Fondacija, Druga Runda Bitke Protiv Masovnog Biometrijskog Nadzora

Share Monitoring, https://bih.bird.tools/data?caseId=2786, 2023.

Share Monitoring, https://bih.bird.tools/data?caseId=2716), 2022.

Statistical Office of the Republic of Serbia, Usage of Information and Communication Technologies in the Republic Of Serbia, 2019.

Statistical Office of the Republic of Serbia, Usage of Information and Communication Technologies in the Republic of Serbia, 2022.

The Republic of Serbia, National Security Strategy of the Republic of Serbia, 2021.

USAID, Serbia Digital Ecosystem Country Assessment, 2021.

Visa, Visa research: Almost a quarter of consumers in Serbia use mobile payments with big potential for digital wallets growth at the market, 2021.

World Bank, Digital Identity for Development, 2021.

Željko S, Slađana S & Slađana B, Digital Transformation of Commercial Banks in Serbia During COVID-19 Pandemic, 2022.