CURRENT CYBER SECURITY CAPACITIES AND DIGITAL RIGHTS IN MONTENEGRO

AUTHORS
Branko Dzakula
Andreja Mihailovic
Nikola Zaric

EDITOR
Ena Bavcic

COPYEDITOR
Marcus Tanner

DESIGN
Igor Vujcic

BIRN
BALKAN INVESTIGATIVE
REPORTING NETWORK

UNDEF
The United Nations
Democracy Fund

FNUD
Fonds des Nations Unies
pour la démocratie

Made possible through support from the UN Democracy Fund

OVERVIEW AND CONTEXT

Montenegro's cybersecurity infrastructure is at a critical point of development and challenge. The country has been actively building its cybersecurity capacities since adopting its first Law on Information Security in 2010. The first National Cybersecurity Strategy was established in 2013, followed by second in 2018 and the latest for 2022-2026[1].

The National Cybersecurity Strategy 2022-2026 highlights the need for integrating advanced technologies, improving response mechanisms to cyber incidents, and strengthening intersectoral and international cooperation to exchange best practices. It also emphasizes the importance of public awareness and education. It calls for continuous efforts to educate the public and private sectors on cybersecurity hygiene and best practices. This includes regular training for employees in public administration and campaigns to raise general awareness about the importance of cybersecurity. Moreover, the strategy sets out clear operational goals, such as enhancing the mechanisms for responding to cyber incidents, improving prevention measures, and establishing a system for protecting critical information infrastructure.

International cooperation is a cornerstone of Montenegro's cybersecurity strategy. The strategy underscores Montenegro's commitment to enhancing its cybersecurity posture amidst evolving threats and its alignment with Western institutions, such as NATO and the European Union. Membership of NATO since 2017 has significantly influenced Montenegro’s cybersecurity policies and strategies, reflecting the importance of cyber defence in national security. Montenegro has ratified several international conventions, including the Budapest Convention on Cybercrime, which it signed in 2009. This convention provides a comprehensive framework for fighting cybercrime, including measures for mutual legal assistance and the harmonization of national laws. In May 2022, Montenegro signed the Second Additional Protocol to the Budapest Convention on Enhanced Cooperation and Disclosure of Electronic Evidence.

Despite this progress, Montenegro has faced a series of sophisticated cyber attacks, revealing persistent vulnerabilities in its digital infrastructure. While the legislative framework has evolved, the corresponding institutional capacity for implementation remains underdeveloped. Cybersecurity enforcement bodies often grapple with resource constraints, both financial and human. The gap between the law and its enforceability exposes Montenegro to heightened cyber risks. To address these challenges, the new Law

[1] Ministry of Public Administration, Digital Society, and Media. (2021). Cyber Security Strategy of Montenegro 2022-2026 with Proposed Action Plan for 2022-2023.

on Information Security[2] aims to establish a robust national framework for managing cybersecurity. It includes measures for achieving a high level of information security for network and information systems, procedures for identifying and determining key and significant entities, and the process for managing cyber security. The law also mandates the establishment of a Cyber Security Agency, responsible for early detection and defence against cyber threats and incidents, coordinating responses during cyber crises, and overseeing the application of security measures in compliance with international standards such as ISO/IEC 27001. The new law's alignment with the EU's NIS2 Directive reflects Montenegrin commitment to adopting comprehensive measures for managing cyber risks, enhancing the resilience of critical infrastructure, and ensuring the continuity of essential services.

The 2023 EU Progress Report[3] stated that Montenegro has substantially increased its capacity to address cybercrime. The number of posts in the specialized unit was increased from 5 to 18, including positions open to IT specialists without a police background. In 2022, the Special Prosecutor's Office launched 11 preliminary investigations for cyber-related offences against 13 people – although there were no final convictions in that year. The capacity of all institutions dealing with cybercrime needs strengthening, particularly regarding the use of electronic evidence in court proceedings.

To investigate the perception of the public and private sector regarding the topic of this study, a research survey was conducted from May 12 to June 6, 2024. During this timeframe, 305 responses were collected from a range of participants, including those from the public and private sectors, academia, international organisations, NGOs and universities. The questionnaire was distributed online as an anonymous survey among a wide audience from the public and private sectors and academia. The research team provided maximum efforts to distribute the survey among employees closely related to cyber security tasks, including both IT and legal aspects of this field. This broad participant base ensured a comprehensive analysis of the cybersecurity landscape in Montenegro.

[2] Proposal of the Law on Information Security of Montenegro. Available at: https://zakoni.skupstina.me/zakoni/web/dokumenta/zakoni-i-drugi-akti/246/3406-19397-10-2-24-1.pdf. Accessed on: June 1, 2024.

[3] European Commission. (2023). Commission Staff Working Document: Montenegro 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions 2023 Communication on EU Enlargement Policy. SWD(2023) 694 final.

CYBER ATTACKS IN MONTENEGRO

Despite its efforts, Montenegro has experienced a series of sophisticated cyber attacks, highlighting ongoing vulnerabilities in its digital infrastructure, particularly in the wake of geopolitical tensions.

A wave of attacks occurred around the parliamentary elections in 2016 that included large-scale Distributed Denial-of-Service (DDoS) attacks on state websites and spear-phishing campaigns aimed at civil servants. The attacks were reportedly orchestrated by the Russian-based group Fancy Bear (APT28), reflecting the geopolitical motives behind these cyber operations.

On August 20, 2022, the biggest cyber attack on Montenegro's institutions that has been registered so far began. It targeted the government's information network and disabled access to governmental websites and email systems, affecting various institutions including courts, the cadastral office and the Revenue and Customs Administration. Network and service restoration continued for weeks, with experts from the FBI arriving to assist in mitigating the impacts. During the attack, all electronic communication between government bodies was halted, as well as communication with businesses and citizens via 5,500 official email addresses.

Detailed analysis revealed ransomware activity and high-level DDoS and Botnet attacks. As a precaution and to prevent further damage, servers hosting the information systems were disconnected from the network. This attack disrupted the smooth operation of public administration, forcing a switch to traditional business methods. Numerous information systems were compromised, affecting service continuity and causing significant damage, necessitating a multi-phase recovery.

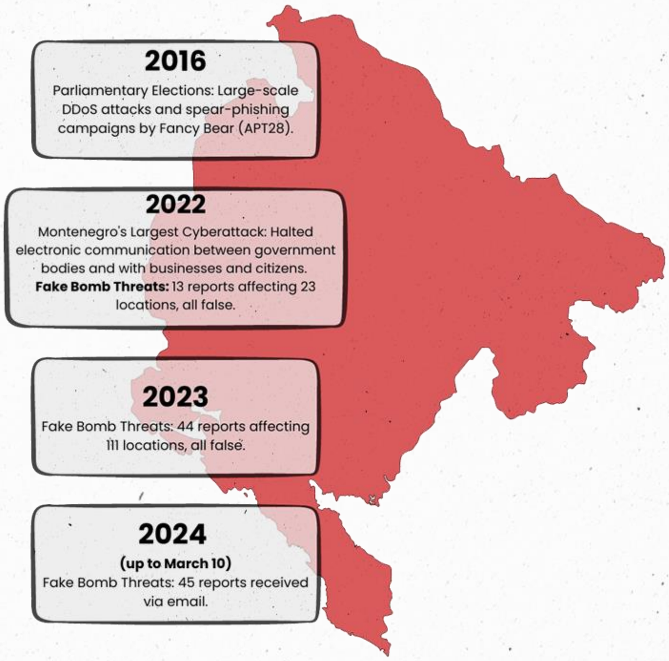
Recovery from the cyberattack was prolonged, with support from both domestic and international partners. An expert team from the United States provided consultative support to overcome the situation and plan better cyber defence mechanisms against future sophisticated attacks. Experts from France's National Cybersecurity Agency (ANSSI) assisted in restoring certain information systems. Experiences were shared with UK partners regarding recent cyberattacks, and joint projects were planned to enhance cybersecurity in Montenegro.

Analysis revealed that 17 information systems across 10 institutions were encrypted, and the cyberattack directly affected 150 computers. One of the key information systems affected was the Social Welfare Information System (ISSS). This system is crucial for processing social welfare applications, issuing individual decisions, conducting monthly reviews and handling payments. The ISSS processes and disburses around 200,000 individual payments monthly, totaling approximately 200 million euros for the year 2023. Disabling this system threatened the livelihood of a significant number of citizens. The ISSS also interoperates with various institutions for data exchange.

The electronic public procurement system was non-functional, delaying public procurements, including essential medical supplies, for several months. The eGovernment portal was down, rendering 383 electronic services unavailable to citizens, legal entities, and the entire administration for a few months. Consequently, the Professional Training Program for 2,743 graduates for 2022-2023 was postponed for a month and the application process for student loans for 3,900 students was delayed. Employment through the electronic candidate testing system was also deferred for two months.

The Government eSession Portal, which supports electronic government meetings and commissions, was out of service, resulting in 10 meetings being conducted on paper. The GOV.ME portal, which publishes information in compliance with the Law on Free Access to Information and updates other essential government data, was non-functional for about a month. The electronic document management system (eDMS) was down for three months, forcing all communication to be carried out on paper.

This attack underscored the critical need for comprehensive cybersecurity measures and the risks associated with geopolitical tensions. In response to these attacks, Montenegro has sought to bolster its cybersecurity defences through international cooperation. The US has played a significant role, providing both financial support and expert assistance. In 2018, the US Cyber Command worked with Montenegrin counterparts to enhance the country's cyber defence capabilities. NATO has also been involved, deploying a counter hybrid team to Montenegro to help deter and manage hybrid threats.



2016

Parliamentary Elections: Large-scale DDoS attacks and spear-phishing campaigns by Fancy Bear (APT28).

2022

Montenegro's Largest Cyberattack: Halted electronic communication between government bodies and with businesses and citizens.
Fake Bomb Threats: 13 reports affecting 23 locations, all false.

2023

Fake Bomb Threats: 44 reports affecting 111 locations, all false.

2024

(up to March 10)
Fake Bomb Threats: 45 reports received via email.

FAKE BOMB THREATS RISE

Montenegro has also seen an increase in fake bomb threats. In 2022, there were 13 threats affecting 23 locations[4]. In 2023, 44 fake alerts impacted 111 locations, and by March 10, 2024, threats had been sent to 45 email addresses. These fake bomb threats caused significant disruption. Law enforcement identified the sources of 16 false alarms delivered via email. This situation underscores the importance of robust security protocols and international cooperation to track and prosecute those responsible.

ANALYSIS OF CYBERSECURITY PERSONNEL IN MONTENEGRO'S PUBLIC SECTOR

Based on publicly available data, Montenegro has been actively working to enhance its cybersecurity capabilities across various public sector institutions. This effort is part of a broader strategy outlined in the National Cybersecurity Strategy 2022-2026, which emphasizes the importance of having an effective response mechanism to cyber incidents and the protection of critical information infrastructure.

Ministry of Interior (MUP)
The Ministry of Interior's specialized units for cybercrime and IT forensics currently include[5]:

- Head of the Cyber Crime and IT Forensics Unit: 1 officer,
- Police Officers for Cyber Crime and IT Forensics: 2 officers,
- Police Officer for Search Activities and Cybercrime: 1 officer,
- Police Officer for Combating High-Tech Crime: 1 officer.

This results in a total of 5 dedicated officers in this unit. These numbers indicate a foundational but limited capacity to address cybercrime, reflecting the need for further investment and expansion. According to Montenegro's Strategy for Cybersecurity 2022-2026, in the coming period, the Police will continue to strengthen its human and technical capacities in the field of cyber security and the fight against cyber crime, as part of which a 100% increase in human resources is planned, as well as the continuation of officer education. In the latest 2023 EU Progress Report, it is stated that Montenegro has substantially increased its capacity to address cybercrime. The number of posts in the specialized unit was increased from 5 to 18, including positions open to IT specialists without

[4] Pobjeda article "In two years, 102 false reports about bombs" Accessed June 10, 2024 https://www.pobjeda.me/clanak/za-dvije-godine-102-lazne-dojave-o-bombama

[5] Source: "RULES ON THE INTERNAL ORGANIZATION AND SYSTEMATISATION OF THE MINISTRY OF INTERIOR AFFAIRS - Podgorica, July 2022"

a police background. Based on the results stated in that report and projections from the Cybersecurity strategy, the Ministry of Interior has overachieved its planned target.

Ministry of Public Administration

The Ministry of Public Administration has a Directorate dedicated to infrastructure, information security, digitalization, and e-services.[6] The personnel includes:

- General Director of the Directorate: 1,
- Directorate Head: 1,
- Heads of Department (System Infrastructure, ICT Infrastructure, Information Security): 3,
- Independent Advisors (various roles): 6.

In total, this amounts to 12 personnel, suggesting a more robust framework aimed at maintaining and enhancing public sector IT infrastructure and security.

Ministry of Defence

The Ministry has also committed substantial resources towards cybersecurity[7]:

- Office Head: 1,
- Independent Advisors (Infrastructure Management, Network Communication, Server Management, etc.): 8,
- Cyber Operations Office Head: 1,
- Cyber Analysts (various levels): 5,
- Montenegro's Defence Advisor at NATO CCD COE: 1.

This brings the total to 17 dedicated personnel, indicating a significant commitment to cybersecurity, particularly in the context of defence and international cooperation. The data from the National Cybersecurity Strategy 2022-2026 focuses on setting targets for increasing the number of personnel dedicated to supporting military operations in cybersecurity. They have set the following targets:

  - ○ 2022: 12 officers,
  - ○ 2024: 16 officers,
  - ○ 2026: 20 officers.

[6] Source: "RULES ON THE INTERNAL ORGANIZATION AND SYSTEMATISATION OF THE MINISTRY OF PUBLIC ADMINISTRATION - Podgorica, June 2022"

[7] Source: "RULES ON THE INTERNAL ORGANIZATION AND SYSTEMATIZATION OF THE MINISTRY OF DEFENSE - Podgorica, July 2022"

National CIRT (Cyber Incident Response Team) - Operating under the Ministry of Defence Data from the National Cybersecurity Strategy highlights an increase in the personnel dedicated to supporting the national cyber incident response efforts . The CIRT has set ambitious targets:

- 2022: 6 officers,
- 2024: 16 officers,
- 2026: 24 officers.

ONGOING CHALLENGES

While the legislative framework has evolved, the corresponding institutional capacity for implementation remains underdeveloped, as cybersecurity enforcement bodies often face resource constraints, particularly legacy systems, limited human capacity, and a lack of comprehensive cybersecurity education. This discrepancy between the law and its enforceability exposes the nation to heightened cyber risks. Additionally, frequent changes in governance structures have led to inconsistencies in cybersecurity policies and practices.

The private sector, especially small and medium-sized enterprises (SMEs), remains particularly vulnerable due to insufficient resources and expertise in cybersecurity. The increasing digitalization of services further exposes vulnerabilities that malicious actors can exploit. According to the ICT Cortex's analysis, the total revenue generated from the ICT sector in Montenegro in 2022 was approximately 602 million euros. This revenue accounted for about 10% of Montenegro's total GDP, which positions the ICT sector as a high priority within the Montenegrin economy, underscoring the potential and commitment of companies to invest in ICT and digital services and products.[8]

There is an observable shortage of skilled cybersecurity professionals within the national workforce. This shortage impedes the country's ability to effectively monitor, detect, and respond to cyber threats, leaving critical infrastructure particularly vulnerable. General awareness and education about cybersecurity are essential for national security. Current efforts to educate the public and private sectors are insufficient, which could lead to vulnerabilities in the network and information systems that are used daily by individuals and corporations. The "UNDP Digital Skills Needs and Opportunities" report highlights a significant level of IT utilization in Montenegro, with statistics that emphasize the necessity for enhanced cybersecurity measures, the protection of digital rights, and robust data protection frameworks. According to the report, 99.4% of companies in Montenegro use computers, and every one of these companies has internet access. This almost universal adoption of basic IT infrastructure underlines the critical role of technology in the business

[8] Cortex ICT. 2023. "Cortex Analyzes the ICT Industry, Achieves Record Numbers." Cortex ICT. Accessed June 3, 2024. https://ictcortex.me/en/cortex-analyzes-the-ict-industry-achieves-record-numbers/#:~:text=Today%2C%20the%20contribution%20of%20this,previously%20mentioned%20data%20and%20parameters.

sector. Furthermore, a substantial 84.6% of these companies maintain an online presence, extending from websites to social media platforms, which underscores the widespread reliance on digital platforms. Despite this high engagement with digital technology, there is a notable discrepancy in specialized IT skills among the workforce—only 32% of employees have specialized ICT skills, which include crucial areas such as cybersecurity. This gap indicates a significant vulnerability within the digital ecosystem of Montenegro, making it susceptible to cyber threats and data breaches.[9]

SURVEY ANALYSIS

General data analysis

Gender equality has been highly achieved with this survey, with 52% of males (156 responses) and 47% of females (136 responses), while 1% (4 responses) preferred not to answer. Regarding the age distribution, 37% were aged 35-44 years and 22.6% between 25-34 years, while 14.8% were between 18-24 and 45-54 years, which provides equality regarding age distribution.

Most of the survey participants were from the private sector with 47.5% (145 responses) and public sector with 32.7% (100 responses), while the rest were from International organisations (3.6%), NGOs (4.2%)~~)~~ and universities (8.2%). This also corresponds to overall employment statistics in related sectors.

The sizes of the entities that survey participants were employed at are more or less equally distributed: 17.7% have less than 10 employees (54 responses), 19.7% have 10-49 (60), 29.2% have 50-259 (89), 18% (55) have 250-999 and 11.5% above 1,000 (35).

Top or middle management participated with 118 responses (38.7%), technicians, administrative staff and associates contributed 125 responses (40.6%) while others preferred not to answer or do not fit these categories.

Considering general data distribution, one may conclude that equality among all categories was achieved and is well balanced.

Part I - Analysis of existing national capacities and vulnerabilities in cyber security

In this part of the survey, questions related to the overall perception of cybersecurity awareness and readiness of employee's organisations are evaluated.

The questions of this part of the survey are given in Table 1, while results are shown in Figure 1.

[9] UNDP Montenegro. 2022. "Digital Skills: Needs and Opportunities." United Nations Development Programme. Accessed June 3, 2024. https://www.undp.org/sites/g/files/zskgke326/files/2023-09/digital_skills_needs_and_opportunities.pdf.

Table 1– Part I questions

No.	Question
1.	How do you rate your organisation's current level of technical and personnel capability to detect and respond to cyber threats?
2.	Does your organisation regularly conduct vulnerability assessments of its network and information systems?
3.	How often does your organisation update its cybersecurity protocols and tools?
4.	Does your organisation have a strategy for managing business continuity in the event of a cyber attack?
5.	Does your organisation have a formally established cyber incident response team?
6.	How would you rate the effectiveness of existing measures to protect against cyber threats within your organisation?
7.	Does your organisation use automated tools to monitor cyber threats?
8.	How quickly can your organisation detect a cyber attack?
9.	Does your organisation regularly collaborate with other entities in the industry to share cyber threat information?
10.	Has your organisation detected a cyber incident?

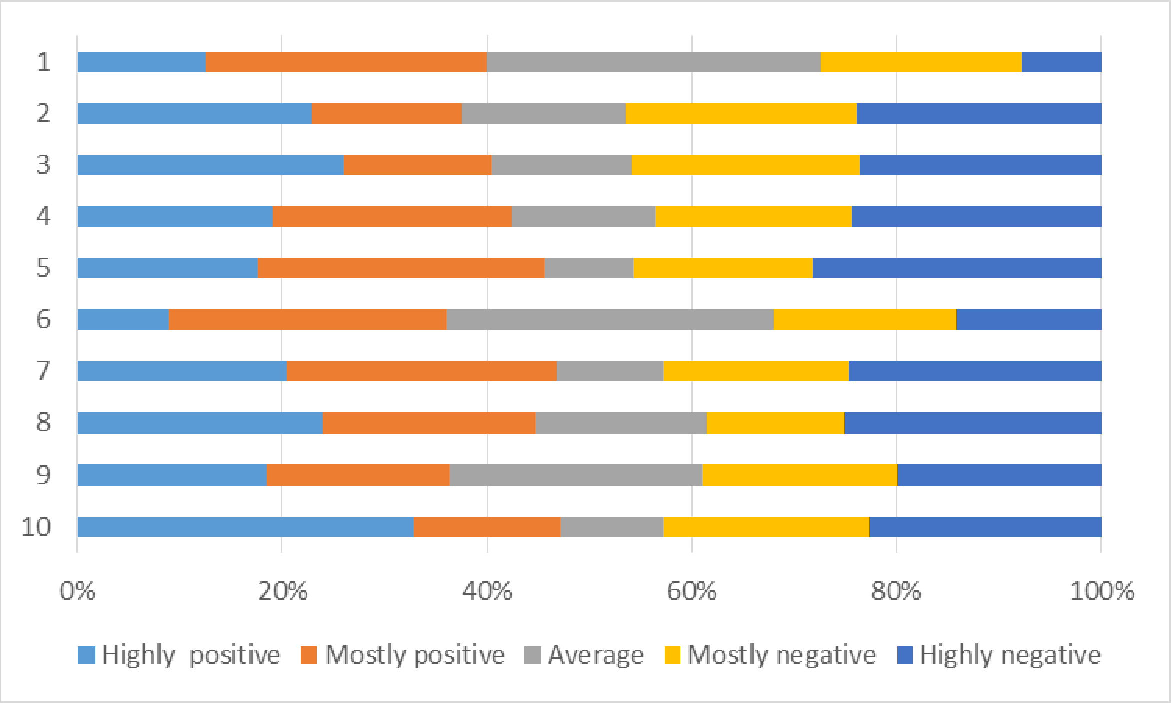


Figure 1 – Statistical overview of Part I responses

Highly and mostly positive answers are provided for all questions in the range of 35%-45%, neutral answers are about 20% with a somewhat higher percentage for questions one and six, while negative or mostly negative answers are provided also in the range 35%-45%. Such results indicate that a number of organisations are highly aware of the importance and necessity of cybersecurity protections and of their readiness to respond to cyber incidents. The response that more than 55% of companies did not detect any cyber incident may indicate that these organisations do not have resources to detect cyber incidents or are now aware what cyber incidents are, since nowadays it is almost impossible that an organisation or individual did not face at least a phishing attack. It is encouraging that about 45% of organizations may detect a cyber attack in less than a few hours.

Part II - Challenges in implementing Law on Information Security

With the new Law on Information Security in the final phase of preparation, the goal of this part of the survey was to investigate how employees and their organisations are informed about its content and the novelties of the law.

The questions of this part of the survey are given in Table 2, while results are shown in Figure 2.

Table 2 – Part II questions

No.	Question
1.	How familiar are you with the content and requirements of the new Law on Information Security?
2.	Do you expect your organisation to be classified as a key or important entity under the new law?
3.	Has your organisation implemented the ISO/IEC 27001 standard?
4.	Do you expect that your organisation will have to significantly increase its information security budget to meet the requirements of the new law?
5.	How do you assess the need to hire external consultants to help implement the new requirements of the law?
6.	Do you expect that the implementation of measures from the law on information security will improve the overall cyber security of your organisation?
7.	What aspects of the new law do you consider the most challenging to implement?
8.	What technical challenges are the biggest obstacles to aligning your organisation with the new law?
9.	Are there specific organisational vulnerabilities that could make it difficult for your organisation to comply with the requirements of the new information security law?
10.	How do you rate your organisation's current capacity to meet the reporting requirements under the new law?

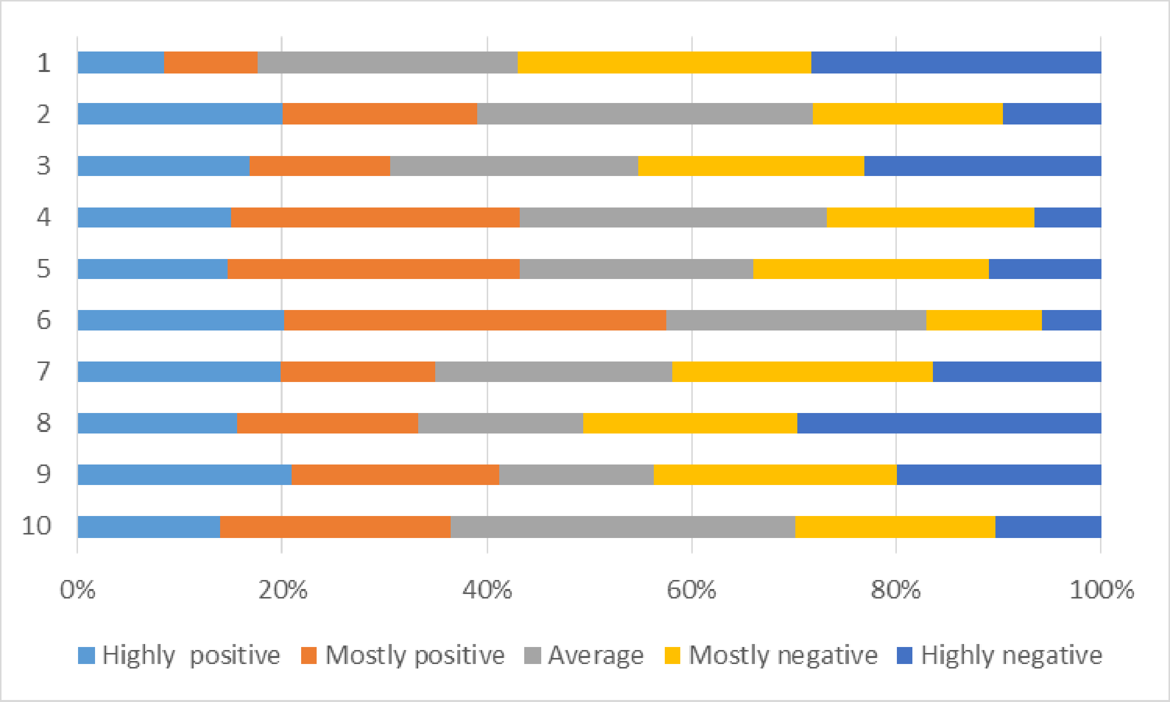


Figure 2 – Responses for Part II

Responses to the first question clearly indicate that the proposal of the new Law of Information Security is not promoted adequately among communities interested in it, which may indicate a lack of transparency in the preparation of the Law proposal. The responses to the other questions are more or less equally distributed, with dominantly mostly positive or average answers.

Apart from the other questions 7, 8 and 9 should be separately considered due to the offered answers that are related to the different aspects of the new Law. The responses to question 7 show that the most challenging parts of the Law draft are requirements for training and education (26%), organisational challenges (23%), technical requirements (20%). Financial and legal aspects are less challenging, with 16% and 15% respectively. Question 8 as the most challenging part of the technical aspect addresses lack of resources or expertise, with 30%. Regarding organisational challenges, only 20% responded that there are no challenges, while insufficient awareness, low organisational culture, lack of clear procedures and limited budget are almost equally distributed.

Part III – Privacy protection and improvement of citizens' digital rights

Part II of the survey is related to the overall perception of the survey participants to the state of cyber privacy and digital rights protection in Montenegro. The questions were related to individual perception, regardless of the sector that participants are employed in. The questions of this part of the survey are given in Table 3, while results are shown in Figure 3.

Table 3 – Part III questions

No.	Question
1.	Do you feel safe using digital services in Montenegro?
2.	Are you familiar with your rights regarding the protection of personal data on the Internet?
3.	Have you ever had the experience of having your personal information misused on the Internet?
4.	Do you believe that organisations and companies in Montenegro take their obligation to protect your personal data seriously?
5.	How do you rate your trust in the digital services provided by the state regarding the protection of your personal data?
6.	Do you think that information about how to protect your privacy and personal data on the Internet is easily accessible and understandable?
7.	Have you ever used legal mechanisms to protect your digital rights or privacy?
8.	Do you think that there is enough education and information about the protection of personal data and digital devices in Montenegro?
9.	Would you support the strengthening of legal measures for the protection of privacy on the Internet in Montenegro?
10.	How do you rate the level of transparency in the processing of personal data by organisations in Montenegro?

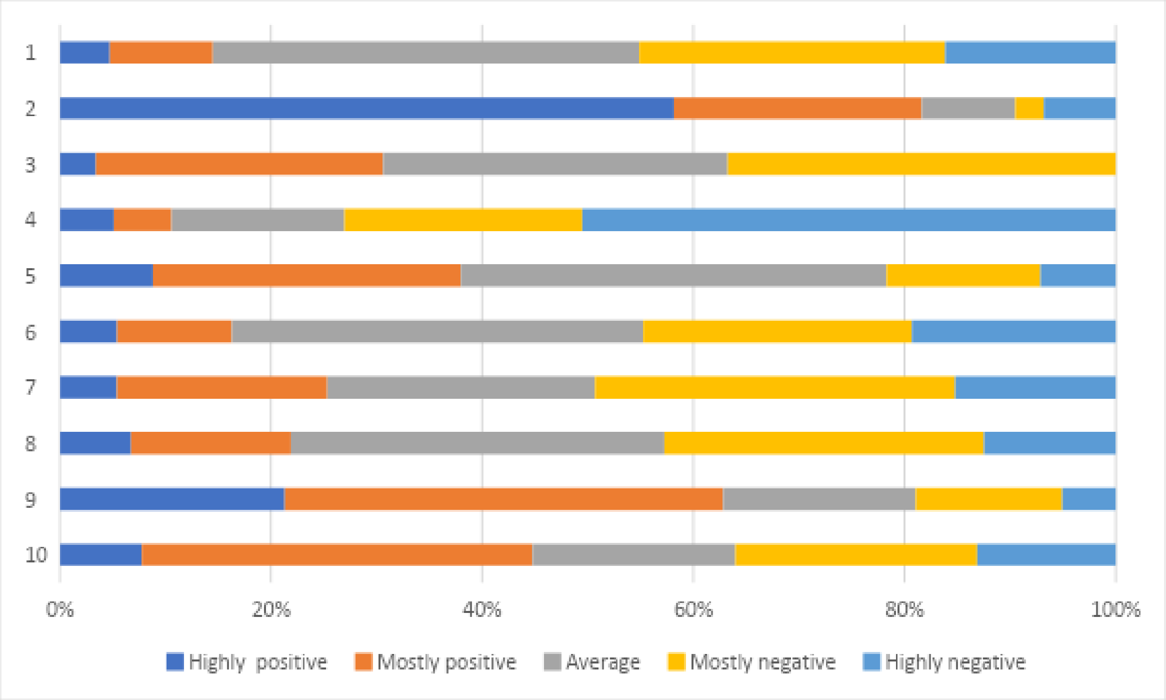


Figure 3 – Responses for Part III

The general perception of safety of using digital services in Montenegro is at a satisfying level, with more that 65% of positive or average answers. An even higher percentage of 82% participants are familiar with rights regarding data protection, meaning that the target group of this survey is very aware about importance of digital rights and safety. This corresponds with the answer to the third question, where less participants experienced misuse of their personal information.

The answers to the next four questions relating to organisations' and companies' capabilities to protect digital rights are quite disappointing. Significant efforts should be made to increase trust and to prove that institutions are capable of protecting digital rights of citizens and companies.

About 70% of the participants think the education availability as well as accessibility of information about personal data protection and digital rights are not sufficient. It is clear that more must be done to increase awareness about importance of education and trainings in the field of digital rights and cyber security.

Since transparency of personal data processing is positively perceived by less than 20% of participants, the response of more than 80%, that stronger legal measures are necessary, is more than expected.

In general a perception about digital rights and data protection exists within the target group, but it is probably much lower in other sectors, and so more should be done to increase general awareness about digital rights and data protection.

Part IV – Education and capacity building in cyber security

The questions of this part of the survey are given in Table 4, while results are shown in Figure 4.

Table 4 – Part IV questions

No.	Question
1.	To what extent are citizens in Montenegro aware of cyber threats and of how to react to incidents?
2.	Have you had the opportunity to participate in cyber security training or education?
3.	How would you rate the effectiveness of cyber security training or education that you have attended?
4.	After previous training or education, did you apply the acquired knowledge in practice?
5.	Which areas do you consider a priority for further improvement through educational programs and support?
6.	Which education model would you prefer to improve your cybersecurity knowledge?
7.	How would you rate the availability of support and resources for victims of cybercrime and violations of digital rights in Montenegro?
8.	Do you think current institutional mechanisms are effective enough in the fight against cybercrime and the protection of citizens' digital rights?
9.	How familiar are you with the possibilities of reporting cybercrime and violations of digital rights to competent institutions in Montenegro?
10.	How would you rate the public's access to information about cyber security and the protection of digital rights provided by institutional mechanisms in Montenegro?

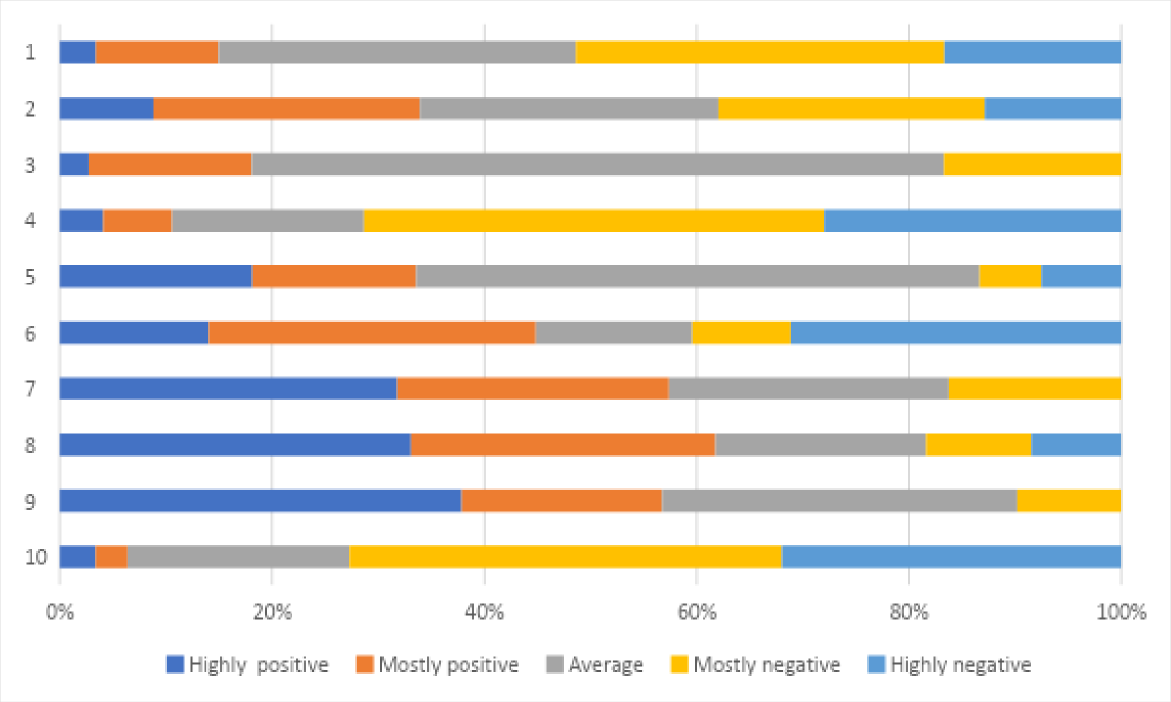


Figure 4 – Responses for Part IV

Maybe the most critical answer in the whole survey is one to the first question in this part, where just 6% assumes that citizens in Montenegro are aware of cyber threats and how to react to incidents. Similar percentages of 12-18% positive answers are for question 7, 8 and 10, related to institutions' capacities to support victims of digital crimes, the effectiveness of institutions against cybercrime and overall access to public data about institutional mechanisms against digital crime. These results are a red alert that something urgently should be done to enhance educational and informative campaigns to increase awareness about private data protection, digital rights and cyber security in general.

Since the survey is conducted mostly within an audience somehow related to cyber security, or at least IT or legal areas, it was expected that almost all of them had participated in some sort of cyber related education, while the survey shows that it was the case for less than 60% of the participants. If the participants could choose the area for education, it would be mainly related to financial fraud and child security on the Internet; business and personal data-related education were not in focus.

CHALLENGES WITH IMPLEMENTATION LEGISLATIVE CHANGES

The proposed Law on Information Security in Montenegro introduces a regulatory framework designed to align with the NIS 2 Directive’s comprehensive approach to achieving a high level of cybersecurity across the European Union. The law's alignment with the NIS 2 Directive is manifest in its structured approach to identifying key and important entities, which is crucial for maintaining a resilient cybersecurity infrastructure. Considering that these entities are instrumental in safeguarding national security framework and maintaining economic and societal functions, the designation of key and important entities as per the NIS 2 Directive principles enhances Montenegro's cybersecurity, by ensuring that these entities implement robust cybersecurity measures.

However, specific challenges regarding implementation and operational efficacy need to be addressed to ensure the effectiveness of this law. Under Article 7 of the NIS 2 Directive, Member States are required to ensure that roles and responsibilities of different national authorities, including CSIRTs, are clearly articulated and delineated to prevent overlaps and ensure effective responses to cyber incidents.

A significant challenge of the proposed law is the lack of clear demarcation of responsibilities between the Ministry of the Public Administration, the Government CIRT and the Cyber Security Agency. Notably, the existing national CIRT, established in 2012 through a joint project between the government and the International Telecommunication Union, is overlooked in the new legislation. The draft instead focuses on a separate Government CIRT within the Ministry of Public Administration, designated solely for state institutions while not addressing the broader scope of key and important entities as emphasized by the NIS 2 Directive.

This approach may lead to inefficiencies, considering the concurrent establishment of a Cyber Security Agency intended to serve as the central body for national cybersecurity. Having in mind the establishment of the National Cyber Security Agency, envisioned as a central body, this dual structure may lead to redundancy and inefficiencies unless clearly defined roles and collaboration mechanisms are established. The NIS 2 Directive, through its provisions on national strategies and the roles of CSIRTs (Articles 7 and 10), advocates for clear and distinct responsibilities to prevent overlaps and confusion. For Montenegro, it may be more pragmatic to consolidate these roles into a single national-level CIRT in order to streamline responsibilities, reduce administrative overhead, resources and potentially increase the effectiveness of cybersecurity responses. Therefore, the proposed law could benefit from re-evaluation of the organisational structure proposed in the draft law, specifying operational boundaries and collaboration protocols between these bodies to comply with these provisions and prevent operational conflicts or duplications.

Additionally, Montenegro faces a challenge in aligning its institutional capacities with the extensive requirements of the new law and needs to focus on developing a robust educational and professional pathway to cultivate a pool of cybersecurity experts capable of managing and mitigating cyber risks effectively and adhere to the law's requirements.

Aligning with Article 5 of the NIS 2 Directive, Montenegro must ensure that these key and important entities are equipped with the necessary resources to meet the law's stringent requirements, which includes developing educational programs and professional training to build a resilient pool of cybersecurity experts. The need to enhance national capacities for cybersecurity incident response is pivotal, as articulated in Article 10 of the NIS 2 Directive that emphasizes the establishment and proper resourcing of Computer Security Incident Response Teams (CSIRTs) that are capable of handling incidents efficiently.

This directive emphasizes the importance of collaboration between government bodies and the private sector, as outlined in Articles 7 and 8, which advocate for the establishment of a strategic framework to enhance national cybersecurity capacities through cooperation across various sectors. Montenegro faces a challenge in aligning its institutional capacities with the extensive requirements of the new law and needs to focus on developing a robust educational and professional pathway to cultivate a pool of cybersecurity experts capable of managing and mitigating cyber risks effectively and adhere to the law's requirements. The collaboration between the public and private sectors can significantly compensate for the existing limitations by pooling resources, sharing joint cybersecurity task forces, platforms for threat intelligence and regular collaboration forums to leverage private sector innovations. This approach is especially vital in a context where state resources alone may not suffice to address the sophisticated and evolving nature of cyber threats. Establishing formal mechanisms for this cooperation is essential in order to integrate the strengths of both sectors to build a resilient national cybersecurity infrastructure.

In conclusion, while the draft law is a step in the right direction, it requires adjustments to fully leverage existing resources like the national CIRT, and to clarify the roles and responsibilities of new and existing entities within the cybersecurity framework. Enhancing public-private cooperation also remains a priority, ensuring that Montenegro not only meets the requirements of the NIS 2 Directive but also establishes a more coordinated, effective, and comprehensive national cyber incident response in alignment with the EU policies.

NEW PERSONAL DATA PROTECTION LAW NEEDED

The potential for significant cyber attacks in Montenegro, evidenced by past incidents, poses a substantial risk to individual privacy and the protection of personal data. Inadequate cybersecurity infrastructure can lead to breaches that compromise personal information, thereby infringing on digital rights. Montenegro’s Personal Data Protection Law[10], adopted in 2008 and last amended in 2017, was enacted before the full implementation of GDPR in the EU. Since its inception, GDPR has set a benchmark for data protection, which Montenegro's existing framework fails to meet. The enactment date of the law is a significant factor, as it

[10] Ministry of Internal Affairs. "Law on Personal Data Protection." Official Gazette of Montenegro, nos. 079/08 (December 23, 2008), 070/09 (October 21, 2009), 044/12 (August 9, 2012), 022/17 (April 3, 2017). Accessed June 3, 2024. https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486.

has not evolved to cover newer concepts of digital rights protection introduced by GDPR. This misalignment suggests that Montenegrin citizens may not enjoy the same robust level of digital rights protection as those in regions compliant with GDPR, potentially compromising their privacy and the security of their personal data.

Firstly, the GDPR mandates that consent for data processing must be freely given, specific, informed, and unambiguous, accompanied by clear affirmative action from the data subject. Montenegro's legislation, however, lacks explicit stipulations regarding the clarity of affirmative consent, potentially leading to ambiguities in whether consent was appropriately obtained. Furthermore, GDPR enhances data subject autonomy by delineating straightforward procedures for withdrawing consent, ensuring that the process of withdrawal is as simple as the process of granting it. This provision is inadequately mirrored in Montenegrin law, where the guidelines for consent withdrawal are less defined, potentially complicating data subjects' control over their personal data. In addition to consent issues, Montenegro's law does not fully embrace the comprehensive rights of data subjects as established under GDPR. Key rights such as access, rectification, erasure ("the right to be forgotten"), and the restriction of processing are only partially covered. Particularly absent is the right to data portability, which significantly empowers individuals by allowing them to receive their data and transfer it to another controller seamlessly. This omission critically limits user control over personal data. Furthermore, the law lacks rigorous protocols for data breach notifications, diverging from GDPR's mandate that such breaches must be reported to relevant supervisory authorities within 72 hours, with affected individuals notified promptly if there is a high risk to their rights and freedoms. This deficiency in Montenegro's framework may delay critical responses to data breaches, exacerbating risks to data security. Also, the current law does not enforce the mandatory appointment of a Data Protection Officer (DPO) for entities that engage in extensive monitoring or processing of sensitive categories of data, a requirement under GDPR that bolsters oversight and accountability. Coupled with insufficient requirements for transparency and record-keeping, these gaps significantly undermine the enforcement capabilities of Montenegrin authorities, hinder compliance monitoring, and pose barriers to the nation's aspirations for EU integration.

These legislative shortcomings not only threaten the digital rights and privacy of Montenegrin citizens but also increase the risk of data misuse and impede the country's progress towards becoming a secure digital economy in line with European standards. The need for a new data protection law in Montenegro is imperative to address the significant gaps in the existing legal framework and align with GDPR. By adopting a new law, Montenegro can enhance its commitment to protecting citizen's digital rights, which is crucial for maintaining public trust in digital services and fulfilling the country's EU accession aspirations. This legislative overhaul will not only improve data protection standards but also strengthen Montenegro's international standing in data security and privacy. In addition, the institutional support for enforcing data protection laws in Montenegro is under-resourced and lacks the technical expertise necessary to monitor compliance effectively, investigate breaches, and enforce penalties comparable to those under GDPR. Alongside legal reforms, initiate comprehensive awareness campaigns to educate both data subjects and controllers about their rights and responsibilities under the new law. This includes training staff in GDPR compliance, increasing transparency in operations, and ensuring adequate funding that will foster a culture of data protection and compliance.

FUTURE DIRECTIONS

The comprehensive survey conducted provides crucial insights into Montenegro's current cybersecurity landscape, pinpointing the disconnect between theoretical frameworks and practical enforcement, particularly in digital rights protection and cyber threat response.

1. Awareness and Education Gaps

The survey identifies a significant lack of broad-based knowledge about digital rights and cybersecurity among the general populace. The data shows that about 55% of organisations had not detected any cyber incidents, which might reflect underreporting or lack of detection capabilities rather than a true absence of incidents. Moreover, with only 6% of citizens aware of how to respond to cyber threats, there is an urgent need for expansive education initiatives. This dichotomy underscores the necessity for comprehensive educational programs that not only cover rights but also practical responses to cyber threats. These programmes should be included in national curricula and supported by ongoing public awareness campaigns that utilize various media channels to reach a broader audience. The government, along with educational institutions, should spearhead national campaigns focusing on digital literacy, specifically targeting rights and protective measures individuals can employ online.

2. Institutional Capacities

The survey results emphasize the inadequacy of current institutional capacities to effectively manage cybersecurity threats and enforce digital rights protections. These constraints are highlighted by the 35%-45% of respondents across various sectors, indicating negative or mostly negative responses regarding the current level of technical and personnel capability to detect and respond to cyber threats. For example, while the Ministry of Defence has dedicated personnel for cyber defence, other critical sectors lag behind, needing urgent reinforcement in both human and technical capacities. There is a clear necessity for increased funding, more specialized personnel, and better technological resources. These investments are crucial to empower the workforce to effectively counter modern cyber threats, as the survey indicated organisational vulnerabilities with a low percentage of entities regularly updating cybersecurity protocols and tools.

3. Public-Private-Academic Partnerships

The survey feedback suggests an underutilization of collaborative opportunities across sectors. A coordinated approach involving government, private sector leaders, and academic institutions can lead to a more resilient cybersecurity infrastructure. Initiatives such as joint cybersecurity task forces and innovation labs would benefit from regular knowledge exchange platforms and shared resources, promoting innovative solutions and best practices in cybersecurity and digital rights protection. Approximately 65% of respondents indicated that their organisations do not regularly collaborate with other entities in the industry to share cyber threat information. This lack of collaboration can hinder the ability of institutions to respond to new and evolving threats effectively. To address the cybersecurity skills gap and accelerate the adoption of cutting-edge protective technologies, there must be a concerted effort to foster collaboration across government, private sector, and academia. Establishing a cybersecurity task force and innovation labs, as well as conducting joint training initiatives, can catalyze the development of robust cybersecurity solutions and ensure a well-rounded approach to safeguarding digital rights.

4. Legal Framework Enhancements

Montenegro has made strides to align with international standards, such as the Budapest Convention and the proposed alignment with the NIS 2 Directive's comprehensive approach, aiming to achieve a high level of cybersecurity across the European Union. The Proposal of the Information Security Law emphasizes the identification and protection of key and important entities that are instrumental in safeguarding national security and maintaining crucial economic and societal functions. However, the survey indicates room for significant improvements in national legislation, as successful implementation of this law is contingent upon addressing existing challenges related to institutional capacities, role demarcation among cybersecurity bodies, and the integration of new educational paradigms. Survey respondents also pointed to ambiguities and gaps in the current legal framework regarding digital rights and cybersecurity. Therefore, the ongoing development of the Law on Information Security is a critical step forward, but it needs to incorporate clear, actionable guidelines and account for the rapid evolution of cyber threats. The law should facilitate easier compliance and enforcement, ensuring that both individuals and organizations have a clear understanding of their responsibilities and rights.

5. Transparency and Reporting Mechanisms

Less than 20% of respondents felt that the processing of personal data by organisations was done transparently. This low level of perceived transparency underscores a significant trust gap between data-handling entities and the public. Given that 70% of survey participants believe that the availability and accessibility of information about personal data protection and digital rights are not at a sufficient level, and more than 80% of participants expressed a need for stronger legal measures to protect privacy on the Internet in Montenegro, it is clear there is a pressing need for improvement in this area. To enhance trust and compliance, Montenegro must improve transparency in how personal data is handled and boost the effectiveness of mechanisms for reporting cyber incidents. This includes integrating 'privacy by design' protocols and regularly conducting impact assessments to adapt to new cyber threats.

To navigate the complex cybersecurity environment effectively, Montenegro must implement a multi-faceted strategy that includes bolstering institutional capacities, enhancing legal frameworks, and fostering an inclusive cybersecurity environment of continuous learning and adaptation. To address these challenges, Montenegro should focus on capacity building and international cooperation. The establishment of a National Cybersecurity Agency and the development of public-private partnerships are seen as critical steps towards enhancing the country's cyber resilience. The pervasive use of digital technologies combined with a shortfall in advanced IT skills highlights an urgent need for comprehensive strategies that focus on enhancing cybersecurity education, updating legal frameworks to protect digital rights and personal data, and fostering closer collaborations between the public and private sectors. Moreover, integrating academic expertise into cybersecurity efforts could provide in-depth analysis and innovative solutions to emerging threats. These measures are essential to safeguard Montenegro's digital landscape, ensuring a secure, resilient, and rights-focused digital environment for all sectors of the economy.

Enhancing institutional capacities should be a priority, focusing on building targeted training programs for government employees and ensuring adequate budget allocations for cybersecurity tools and training. Strengthening the national CSIRT (CIRT.ME) is critical, involving the provision of advanced tools and continuous training to improve rapid threat detection and response while setting up clear segregations of duties and responsibilities between the new Agency for Cybersecurity and the national CIRT. Collaboration with EU cybersecurity bodies, particularly the European Union Agency for Cybersecurity (ENISA), can provide technical assistance and capacity-building programs to ensure Montenegro's cybersecurity efforts align with EU standards.

The analysis of cybersecurity personnel across key public sector ministries in Montenegro indicates a deliberate effort to enhance national cybersecurity capacities. Notable examples include the Ministry of Defence, with 17 dedicated personnel, and the Ministry of Public Administration's with 12 personnel. This indicates a need to enhance capacities by increasing the number of employees working on cybersecurity and cyber defence for a proactive approach to scaling cybersecurity defences in response to evolving threats

Public-private-academic collaboration is essential to address the cybersecurity skills gap. Establishing a cybersecurity task force that includes government officials, private sector leaders and academic experts can facilitate regular information sharing and the development of best practices. Joint training initiatives with universities and private companies should address specific skills gaps, directly meeting staffing requirements of the public and private sectors. Promoting cybersecurity innovation labs in partnership with tech companies and academic institutions can focus on developing new technologies and strategies to safeguard digital rights.

Addressing cybersecurity and privacy challenges requires national awareness campaigns to educate the public about best practices and the importance of protecting personal data. Enhancing mechanisms for reporting cyber incidents and ensuring transparent communication about breaches is crucial for maintaining public trust. Integrating ‘privacy by design’ principles into all digital services will proactively enhance user trust and compliance with privacy standards. Establishing a monitoring body to oversee Montenegro’s alignment with EU cybersecurity standards and integration goals will support the country’s EU accession aspirations.

Montenegro’s gradual increase in cybersecurity personnel and strategic efforts across various ministries reflect a commitment to bolstering national cybersecurity capacities. A continuous focus on training, resource allocation, and inter-sectoral collaboration will be vital to addressing the challenges and meeting the objectives outlined in the National Cybersecurity Strategy 2022-2026. By adopting these comprehensive measures, Montenegro can strengthen its cybersecurity infrastructure, protect digital rights, and build resilience against evolving cyber threats.

In conclusion, while Montenegro has made significant strides in developing its cybersecurity framework, ongoing geopolitical tensions and evolving cyber threats necessitate continuous improvements and international collaboration. The lessons learned from past incidents highlight the importance of a proactive and comprehensive approach to cybersecurity, starting with addressing the cybersecurity skills gap.

RECOMMENDATIONS

1. Enhancing Institutional Capacities

a. Capacity Building for Public Institutions: Develop targeted training programmes for employees within key government agencies responsible for implementing the new law. This includes intensive workshops on the latest cybersecurity trends, the NIS 2 Directive requirements, and incident response protocols.

b. Strengthening National CSIRT: Enhancing the capabilities of Montenegro's national CSIRT is critical. By providing advanced tools and specialized training, the CSIRT will be better equipped for rapid detection and response to cyber threats, a cornerstone for protecting digital rights and privacy.

c. Technical Assistance from EU Bodies: Seek technical assistance and capacity-building programs from EU cybersecurity agencies. This can include partnering with the European Union Agency for Cybersecurity (ENISA) to leverage their expertise in bolstering national cybersecurity frameworks.

2. Public-Private-Academic Collaboration

a. Tripartite Cybersecurity Task Force: Establish a task force that includes representatives from the government, private sector and academic institutions to focus on enhancing cybersecurity infrastructure and sharing knowledge on best practices and technological advancements.

b. Joint Cybersecurity Training Initiatives: Collaborate with universities and private sector entities to develop comprehensive cybersecurity training and education programmes that address specific skills gaps identified within public institutions.

c. Innovation Labs and Research Partnerships: Promote the creation of cybersecurity innovation labs that partner with tech companies and universities. These labs can focus on developing new technologies and strategies to safeguard privacy and enhance digital rights protection.

3. Legal and Regulatory Framework Enhancement

a. Regulatory Sandbox for Cybersecurity Solutions: Implementing a regulatory sandbox will allow both local and international companies to test innovative cybersecurity products and solutions within a controlled environment. This ensures that new technologies align with Montenegro's legal standards before full-scale deployment.

b. Continuous Legal Update Mechanism: A legislative review committee should be established to periodically assess the effectiveness of the cybersecurity law. This committee will propose necessary amendments to address emerging digital threats and ensure continuous alignment with EU standards.

4. Addressing Cybersecurity and Privacy Challenges

a) Cybersecurity Awareness Campaigns: National campaigns to raise awareness about cybersecurity practices and the importance of protecting personal data are vital. These campaigns will educate the public on the implications of digital vulnerabilities on privacy and digital rights.

b) Enhance Incident Reporting and Transparency: Improving mechanisms for reporting cyber incidents will ensure timely and transparent communication about breaches. This transparency is essential for maintaining public trust and effectively managing the impact on personal data and privacy.

c) Privacy by Design Protocols: Encouraging the adoption of 'privacy by design' protocols for all digital services will ensure that privacy safeguards are integrated into technologies from the onset.

5. Monitoring and Evaluation

a) Regular Impact Assessments: Conduct regular assessments to evaluate the impact of cybersecurity measures on digital rights and privacy, adjusting policies and strategies based on these findings.

b) EU Integration Pathway Monitoring: Establish a monitoring body specifically focused on aligning Montenegro's cybersecurity efforts with its EU accession goals, ensuring that digital rights protections are consistent with EU standards.

ANNEX I

Research Plan:

As part of the BIRN Digital Rights program and ongoing efforts aimed at enhancing the level of cybersecurity and the protection of digital rights in Montenegro, a multidisciplinary research team (comprising Branko Džakula from UN1QUELY Cybersec Academy, Dr Andreja Mihailović from LF UoM, and Prof Dr Nikola Žarić from FEE UoM) conducted a study with the goal of evaluating existing capacities, identifying key vulnerabilities, and analyzing the level of citizens' awareness of privacy protection and their rights in the digital environment.

Research Objective: The planned study aimed to provide a comprehensive analysis of national capacities in the field of cybersecurity and digital rights protection in Montenegro, which is becoming increasingly relevant due to rapid changes in the digital landscape, the national cyber index, the growing frequency of cyber incidents, and forthcoming regulatory changes. Montenegro has been actively building its cybersecurity capacities since the adoption of its first Law on Information Security in 2010, including the development of the National Cybersecurity Strategy 2022-2026 which highlights the need for the integration of advanced technologies, enhancement of response mechanisms to cyber incidents, and strengthening of intersectoral and international cooperation to exchange best practices. This is particularly relevant in the context of recent cyber incidents in August 2022, which highlighted potential weaknesses in the national cyber infrastructure, causing significant systemic delays in the functioning of state organs. The research would identify how various organisations in the public, private, and civil sectors in Montenegro manage cyber threats and protect individuals' rights in the digital space. A specific focus will be on the capacity analysis for the implementation of the ISO 27001 standard in light of the new Law on Information Security in accordance with the NIS2 directive. Considering that the national cybersecurity strategy emphasizes the need for continuous education and training of personnel to respond to increasingly complex challenges in the digital environment, the research would also provide guidelines for the development of training programs and certification in collaboration with academic institutions and relevant business partners to fill the existing gap in the labor market.

Methodological Approach: The research would be conducted through quantitative and qualitative data collection using specially designed questionnaires, relevant reports, publicly available records, and analysis of the existing legislative and strategic framework.

Expected Impact: The research not only addresses current needs but also anticipates future challenges, making it instrumental for strategic planning of the national framework for cybersecurity and the protection of individuals' digital rights in Montenegro. The results of this study will provide key insights into the capacity of organizations in Montenegro to take steps to strengthen their cyber infrastructure and align with European standards in the fields of cybersecurity, privacy, and digital rights of individuals.

Key Research Areas:

Analysis of Existing Capacities and Vulnerabilities: Focused on assessing the current capabilities of key actors in Montenegro to detect, respond to and prevent cyber incidents. This analysis included identification of systemic vulnerabilities, the assessment of available resources for cyber defense, and the analysis of the effectiveness of existing cybersecurity protocols and practices.

Challenges in Implementing Legislative Changes: Analysis of the challenges organisations face in aligning with the new legislative framework, including the new Law on Information Security aligned with the EU's NIS2 directive. The law, expected to be adopted in 2024, mandates the implementation of the ISO 27001 standard for key and important entities, further emphasizing the significance of this research for enhancing national cyber capacities.

Protection of Privacy and Digital Rights: Evaluation of the awareness of citizens and organisations about privacy protection and digital rights, as well as the impact of current practices on citizens' trust in digital services. This segment includes an analysis of the effectiveness of personal data protection mechanisms and their application in practice in light of international standards and national laws.

Labour Market Situation and Workforce Needs Analysis: The research would cover an analysis of the current state of the labour market in the field of cybersecurity, identification of missing competencies, and the need for additional education and training. According to publicly available records, there is a pronounced need for qualified personnel to apply information security measures, manage cyber incidents, implement security standards and protocols, and understand regulatory frameworks such as GDPR and the NIS2 directive.

Research Phases:

Questionnaire Design and Preparation: Development and validation of a questionnaire focused on key aspects of cybersecurity and digital rights, designed for the needs of the research in collaboration with field experts and legal advisors to ensure relevance and legal compliance.

Distribution and Data Collection: The questionnaire was distributed electronically to employees in the public, private, and civil sectors in Montenegro. This step also involved encouraging participants through a motivational campaign highlighting the significance of their contribution to the evaluation of national capacities, as well as the availability of a toolkit aimed at raising awareness in the field of cybersecurity.

Data Analysis and Reporting: Application of quantitative methods to analyze the collected data, and formulation of recommendations for the enhancement of national policies. The results would be synthesized in a report that will be available to decision-makers, research participants, and the public.

ANNEX II

Survey description and methodology

The survey created for the purpose of this research has 45 questions, divided in five parts;

- Introduction - General data – 5 questions

- Part I - Analysis of the existing national capacities and vulnerabilities in the cyber security area – 10 questions

Part I entails a thorough assessment of the capabilities that key actors possess to detect, respond to, and prevent cyber incidents. It includes identifying systemic vulnerabilities, evaluating the resources available for cyber defence, and analyzing the effectiveness of current cybersecurity protocols and practices. Results from the survey indicate a spectrum of readiness levels among organizations, with a balanced mix of positive, neutral, and negative perceptions regarding cybersecurity preparedness.

- Part II - Challenges in implementing the Law on Information Security – 10 questions

Part II involves examining the hurdles organisations encounter while aligning with the new legislative framework, particularly the upcoming Law on Information Security which integrates the EU's NIS2 directive. This law mandates the adoption of the ISO 27001 standard among crucial entities and is poised to significantly influence the national cybersecurity landscape. Survey findings suggest a substantial gap in awareness and preparedness for these changes, emphasizing the need for improved communication and training to facilitate smoother implementation.

- Part III - Privacy protection and improvement of citizens' digital rights – 10 questions

Part III evaluates how well citizens and organisations understand and protect privacy and digital rights. This segment also assesses the impact of current practices on citizens' trust in digital services and the effectiveness of personal data protection mechanisms in compliance with international standards and national laws.

- Part IV - Education and capacity building in cyber security – 10 questions.

Part IV examines the current state of the cybersecurity labour market. It identifies gaps in competencies and underscores the urgent need for additional education and training. The demand for qualified personnel to manage cyber incidents, implement security protocols, and navigate regulatory frameworks like GDPR and NIS2 is particularly highlighted, reflecting a critical area for future development in the cybersecurity field in Montenegro.

Five answers were available to each question and could be classified as:

- 1. Highly positive (responses like: yes, very frequently, in real time, very well informed)
- 2. Mostly positive
- 3. Average
- 4. Mostly negative
- 5. Negative (responses like: no, very rare, not at all, not informed).