



Montenegro Elections Cybersecurity Report

Assessment and
Recommendations

Editors: Priit Vinkel and Maili Kark
Design: Dada
Proofreading: Refiner
Copyright© e-Governance Academy
2023



**Funded by the
European Union**

This publication has been produced with the assistance of the European Union within the project „Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia“. The contents of this publication are the sole responsibility of its authors and can in no way be taken to reflect the views of the European Union.



The e-Governance Academy is an Estonian centre of excellence to increase the prosperity and openness of societies through digital transformation. In 20 years, we have cooperated with more than 280 organisations from 141 countries, supporting a more efficient use of information and communication technologies in governance and democratic processes. The core of our team consists of the architects and founders of the Estonian and Ukrainian e-state. More information: ega.ee



Montenegro Elections Cybersecurity Report

Assessment and
Recommendations

Contents

List of Acronyms	4
Preface	5
1. Executive Summary	6
2. Methodology	9
3. Background and Context	10
Why is This Topic Important?	10
Election Management in Montenegro and Key Cybersecurity Stakeholders	12
Election Management Stakeholders	12
General Cybersecurity Stakeholders	13
Cybersecurity Legal Framework	14
4. Assessment of the Election Management ICT Infrastructure	16
Context of the Election Management ICT Infrastructure	16
Threats and Security Measures for the Voter Register	18
Threats and Security Measures for Election-Related Web Pages	19
Threats and Security Measures for Voter Identification Devices	21
5. Risks and Recommendations	23
High Criticality Risks	23
Medium Criticality Risks	25
Annex	27

List of Acronyms

AFIS – Automated Fingerprint Identification System

CIRT – Computer Incident Response Team

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial-of-Service Attack

DNS – Domain Name System

EMB – Electoral Management Body

ICT – Information and Communication Technology

IFES – The International Foundation for Electoral Systems

ITU – International Telecommunication Union

GSOC – Government Security Operations Center

MEC – Municipal Election Commission

MFA – Ministry of Foreign Affairs

MoI – Ministry of Interior

MoD – Ministry of Defense

MPA – Ministry of Public Administration

NSA – National Security Agency

ODIHR – OSCE Office for Democratic Institutions and Human Rights

OSCE – Organization for Security and Co-operation in Europe

SEC – State Election Commission

SSL – Secure Sockets Layer

TLS – Transport Layer Security

VR – Voter Register

Preface

This report is compiled within the project “Cybersecurity Rapid Response for Albania, Montenegro, and North Macedonia” (NDICI CRISIS FPI/2022/435-117), funded by the European Union and conducted by the e-Governance Academy. One of the project’s main aims is strengthening governance structures and improving cybersecurity incident and risk management in Montenegro.

This assessment offers an overview of the election management ICT infrastructure in Montenegro and proposes recommendations for risk mitigation.

Montenegro has suffered numerous cyber incursions aimed at public sector institutions. Therefore, examining election management information technology readiness and cybersecurity resilience is of the utmost importance. This assessment offers an overview of the election management ICT infrastructure in Montenegro and proposes recommendations for risk mitigation. The e-Governance Academy would like to extend its appreciation for the valuable input and positive cooperation with representatives from the Montenegrin public sector, private sector, civil society, and academia during the drafting of the report.

The recommendations were presented to key stakeholders in the Montenegrin ICT community and discussed at an election cybersecurity workshop on June 13, 2023, in Podgorica.

1. Executive Summary

Following the August 2022 cyberattacks on Montenegro's national information infrastructure, most key national stakeholders became more aware of the urgency of improving national cybersecurity posture, notably national institutions' capacities and interagency coordination. This has led to some positive developments, such as the de facto establishment of a governmental CSIRT (GOV CIRT) within the Ministry of Public Administration (MPA) and the employment of a number of new cybersecurity specialists.

Moreover, the MPA drafted amended cybersecurity legislation that envisaged the establishment of a new Cybersecurity Agency under the Montenegrin Government and a new national cybersecurity governance setup. However, the draft law was withdrawn from the parliamentary procedure, and its adoption and implementation will be decided following the 2023 parliamentary elections. Nonetheless, existing authorities and national experts continue to be committed to implementing improvements and furthering national capacities for cybersecurity resilience.

Even countries that use limited technology in elections, such as Montenegro, face cyber risks to electoral integrity that require serious consideration.

Although there are no cases of explicit targeting, dealing with cybersecurity issues – particularly in the framework of electoral processes and election infrastructure – has become a vital necessity. Potential cyber incidents before, during, and after elections have very prominent and wide-reaching effects and receive increased public attention. Even countries that use limited technology in elections, such as Montenegro, face cyber risks to electoral integrity that require serious consideration. All electoral processes depend on technology to some degree, including the voter, party, and candidate registers and the processing and publication of results.

The key stakeholders in the Montenegrin electoral management ICT infrastructure are the Ministry of Interior (MoI) and the State Election Commission (SEC), supported by a wide array of institutions like the Ministry of Public Administration (MPA), the Ministry of Foreign Affairs (MFA), local municipalities, the Parliamentary Service, and others. Unofficially, several civil society organizations, such as the Center for Democratic Transition (CDT) and the Center for Monitoring and Research (CeMI), hold a meaningful role in the broader electoral management scope, acting as the main source of electoral information for the public during the preliminary result dissemination phase after election day.

The critical components in the election ICT infrastructure in Montenegro fall into three categories.

- 1) First is the main voter registration database for storing voter identity and authentication on election day.
- 2) Second, several web pages and services for checking public voter data (biraci.me), the verification of signatures in support of election lists (provjeripotpis.me), and a general page for official voting results and election information (dik.co.me).
- 3) Third, special dedicated voter identification devices (the hardware and software) are used in polling stations on election day.

The responsible authorities have already introduced and implemented a number of security measures in the three election ICT infrastructure categories (e.g., voter data encryption for transfer, access restrictions to databases, firewall protection, and DNS [Domain Name System] location-based access to some web pages).

However, numerous risks remain to be mitigated.

Most importantly, there is a lack of precise and systematic rules of engagement, no clear regulation for regular improvement plans, cases of outdated and vulnerable software solutions, very general risk evaluation and crisis plans, a lack of detailed security policies for web page management, and a very limited official election result reporting system. Additionally, there is a shortage of specialized election ICT personnel and a need for more general cybersecurity risk awareness.

Based on the analysis of the current state of Montenegro's election infrastructure, eight risks (five of which are considered high and three medium, in terms of critical importance) were described, and recommendations for possible mitigation measures were outlined (more detailed explanations can be found in Chapter 5).

Risk No. 1 **Criticality: high**



IT infrastructure lacks precise rules for guaranteeing cybersecurity that should be implemented thoroughly and systematically for all election-related systems and components. Regular auditing, testing, and plans for improvement are not specified in regulations and policies.

Recommendations:

1. Regular security audits and tests should be conducted.
2. A dedicated task force with a clear and transparent chain of command should be set up to encounter possible election ICT-related incidents quickly.
3. Uniform cybersecurity policies and procedures should be in place (e.g., for networks and computers).
4. Limited and controlled user access and a clear user policy in place.
5. User activity in election-related databases should be logged and monitored.

Risk No. 2 Criticality: high



Outdated software causes systems and web pages to be vulnerable to malicious activities.

Recommendations:

1. Regular software updates and server patching should be the norm.
2. Use licensed or controlled open-source software and ensure timely renewals.

Risk No. 3 Criticality: high



No sufficiently detailed risk evaluation or crisis plans.

Recommendations:

1. Risk evaluation and compulsory incident notification policy has to be implemented.
2. Crisis management, response, and communication plans need to be drafted.
3. Guidelines, drills, and simulations for cyber hygiene have to be prepared, and relevant good practices presented.

Risk No. 4 Criticality: high



A lack of security rules and policies for voter information and web page management can compromise sensitive voter data.

Recommendations:

1. Websites activity logging and monitoring have to be implemented.
2. Data validation and encryption methods should be applied.

Risk No. 5 Criticality: high



A lack of official vote tabulation and reporting system and inconsistencies in displayed results could erode trust in official results.

Recommendations:

There has to be a unified official structure for vote tabulation and results display, if possible, by using open data principles.

Risk No. 6 Criticality: medium



A lack of broad-based cybersecurity and cyber hygiene training could raise risks of harmful incidents.

Recommendations:

1. Enhance the overall awareness of cyber threats.
2. Hold regular cybersecurity awareness training for personnel using/accessing election-related databases.

Risk No. 7 Criticality: medium



Physical security measures of voter identification devices are unclear between elections.

Recommendations:

The devices' physical security between elections must be regulated in more detail.

Risk No. 8 Criticality: medium



There is a deficit of specialized IT personnel in election management.

Recommendations:

Create a community of all election stakeholders.

2. Methodology

The data for this report was collected via interviews with key stakeholders, a study of Montenegrin legislation on cybersecurity and elections, following and observing the electoral procedures in the Montenegrin presidential elections held on March 19, 2023, and April 2, 2023, and parliamentary elections held on June 11, 2023, monitoring media reports, and desk research.

Meetings and interviews were conducted with representatives from the State Election Commission, the Ministry of Interior, the Ministry of Public Administration, and civil society and academia stakeholders. Supplementing meetings were held with international elections and electoral technology experts who are well-informed about the electoral management of Montenegro.

Two project team members were registered by the SEC as official election observers. These team members followed the voting procedures and tabulation of results at the parliamentary elections held on June 11, 2023. Additional input was gained in preparing and conducting the election-themed cybersecurity table-top exercise held on March 24, 2023, in Podgorica. This report's preliminary recommendations were discussed and validated at the Podgorica Election Security Workshop on June 13, 2023. Both events attracted many experts and stakeholders from the public sector and private companies.

3. Background and Context

Why is This Topic Important?

Elections are crucial to the functioning of a representative democracy. Compromises in the election processes can delegitimize the whole political system. At the same time, elections have become an increasingly frequent target in the modern digital era. Cyberattacks – often combined with information operations and other hybrid threats – are a reality in elections. Even countries that use limited technology in elections face cyber risks to electoral integrity that require serious consideration. All electoral processes depend on technology to some degree, including voter, party, and candidate registers, results processing, and the publication of results.

Dealing with cybersecurity issues, particularly in the framework of electoral processes and election infrastructure, has become a vital necessity. Cyber incidents before, during, and after elections have prominent and wide-reaching effects and receive increased public attention. Electoral processes are backed and enhanced by digital solutions throughout the electoral life cycle (this is also valid in instances where the voting process itself is not carried out in any digital form), ranging from voter roll promulgation, data exchange with the campaigns, poll worker training, voter registration in the polling station, to the correct publication of electoral results, statistics, post-election audits, and the appeal process.

Compromises in the election processes can delegitimize the whole political system.

According to an International Foundation for Electoral Systems (IFES) compendium on cyber threats and vulnerabilities in elections from 2022,¹ the most vulnerable targets in the electoral ecosystem are:

- all informational and dissemination-oriented websites;
- voter rolls;
- voting machines and mechanisms;
- vote tabulation equipment;
- results announcement processes and candidate/party databases.

The three most common attack vectors are identified as:

- disruption or denial-of-service attacks;
- data phishing attempts;
- ransomware assaults on public targets (incl. election-dedicated).

The Estonia/Czechia-led election security compendium from 2018² also noted the risks of large-scale defacing and the misconfiguration of public web resources during the electoral period.

1 See <https://www.ifes.org/publications/cybersecurity-fundamental-elections>

2 See <https://www.ria.ee/media/739/download>

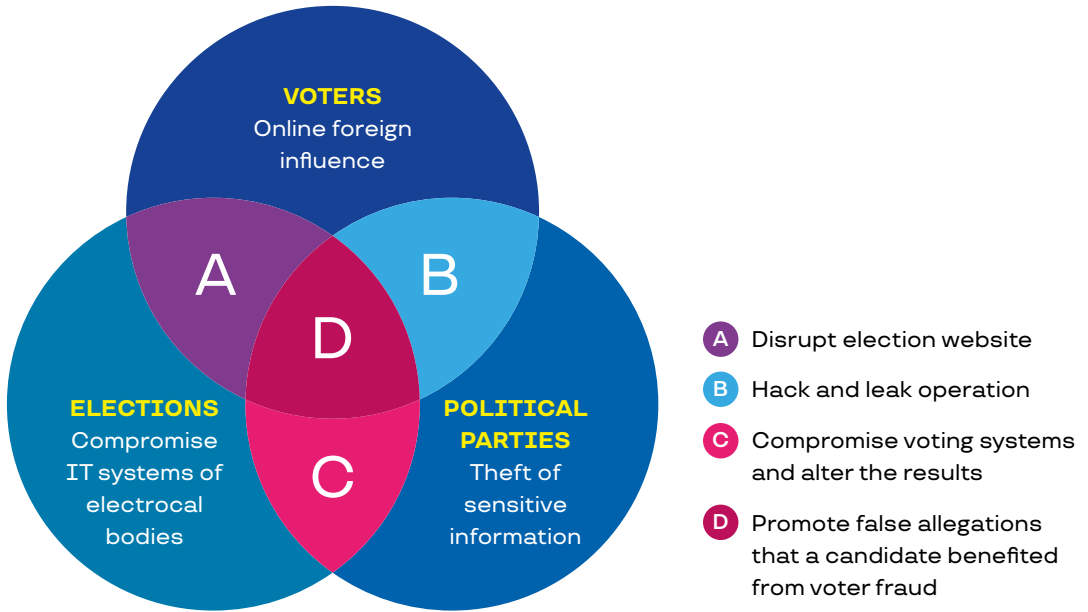


Figure 1. Multiple targets of cyber threat activity during elections.

Source: Canadian Centre of Cyber Security (2021)

The number of digital service or device-related stakeholders in the electoral life cycle is large and multi-faceted and includes dedicated electoral personnel (election management bodies, EMBs), public sector cybersecurity service providers, parties, candidates, and the wider public. Additionally, any possible hardware and software providers from the private sector become relevant stakeholders regarding this topic (see also Figure 1).

Some possible measures for addressing and preventing election-related cyberattacks are the following:

- risk mitigation mechanisms, crisis management plans, incident detection, and response plans;
- awareness raising and training activities among the different stakeholders, also the public (especially cyber hygiene properties);
- specialized cybersecurity training for stakeholders (incl. parties and candidates);

- enforcing cybersecurity guidelines to all vendors and intake services;
- requirements for security testing, auditing, and penetration controls;
- prioritizing election security as a whole-of-government process and inter-agency networking assignment, i.e., the International IDEA publication on Cybersecurity in Elections from 2019.³

³ See <https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf>

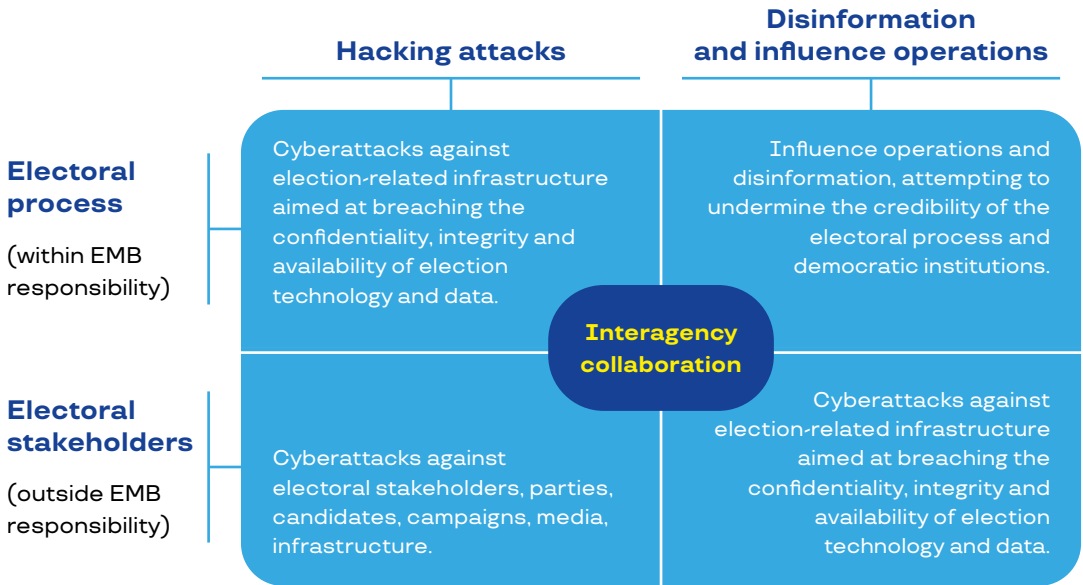


Figure 2. The role of election management bodies (EMB) and other stakeholders in electoral cybersecurity.

Source: International IDEA (2019)

Election Management in Montenegro and Key Cybersecurity Stakeholders

Election Management Stakeholders

The electoral management structure of Montenegro is multi-tiered and consists of a hierarchy of the State Election Commission, the municipal election committees, and the polling station committees.

The **State Election Commission (Državna izborna komisija, SEC)** is the central authority in Montenegro responsible for overseeing and managing the electoral process at the national level. It consists of members appointed by political parties and other societal stakeholders. According to electoral law,⁴ the primary duties of the SEC

in the context of the technical management of an election include responsibility for the development and maintenance of voter register(s) (technological development and maintenance are provided by the Ministry of Interior), management of candidate lists submitted by political parties and coalitions (incl. signature management), and the training and education of the staff of municipal election commissions and polling station committees. Additionally, the Parliamentary Service of Montenegro provides everyday internet-related services to the SEC (e.g., the official web page).

Additionally, the SEC is responsible for the logistic management of elections, including voter identification devices and the accompanying security equipment, in addition to traditional election materials (e.g., ballots, boxes, etc.). The SEC is also responsible for receiving and addressing complaints and appeals related to the electoral process. It

⁴ See <https://dik.co.me/wp-content/uploads/2021/04/Zakon-o-izboru-odbornika-i-poslanika.pdf>

has a role in informing the public about the electoral process, voters' rights, and responsibilities and ensuring transparency and public trust in the electoral process and the technical features used.

The 25 **municipal election commissions (MECs)** manage the election organization, conduct, and results tally in their respective area and ensure the management of polling stations.⁵

The **Ministry of Interior (MoI)** plays a significant role in the technology-related electoral management of the country as it is responsible for maintaining and providing the cybersecurity of the biraci.me website, which is a dedicated public access point for verifying personal voter register data. The MoI is also responsible for maintaining the voter list IT infrastructure, voter database, ID devices for electronic voter identification, and the AFIS system for deduplicating voters' fingerprints in the dedicated database.

Unofficially, several **civil society organizations**, such as the Center for Democratic Transition and the Center for Monitoring and Research, bore a meaningful role in the broader electoral management scope of the observed 2023 elections. The official channels of the SEC and other election management bodies provided the first officially sourced preliminary election result data two days after election day. The election evening data offered to the public in the media was exclusively provided by civil society organizations and based on parallel tally and projections. Therefore, civil society organizations inadvertently provide information, transparency, and engagement for the broader public in the tallying process on election night.

General Cybersecurity Stakeholders

The **Ministry of Public Administration (MPA)** proposes and implements policies to develop the information society. It prepares

draft laws and other regulations in the field of information security and provides expert assistance for applying information and communication technologies in public administration and other state bodies.

To improve the organization of cybersecurity at the network level of government bodies managed by the MPA, following cyberattacks on the government's IT infrastructure and information-communication network in August 2022, a particular organizational unit called the Directorate for Information Security has been formed within the Government Security Operations Center (GSOC). An advanced cybersecurity ecosystem has been established, and a set of tools necessary for efficient threat detection, response, and damage prevention system for assets and data has been implemented.

CIRT.ME (the national CSIRT within the Directorate for the Protection of Classified Information) is responsible for handling security incidents involving information technology in the cyberspace of Montenegro. It was formed in 2012 as part of a joint project between the Government of Montenegro and the International Telecommunication Union (ITU). Until November 2020, CIRT was under the MPA, but after amendments to the Law on Data Secrecy, it became the responsibility of the Directorate for the Protection of Classified Data. The function of the national CIRT is to protect national networks from incidents related to computer security arising from the internet and other information security risks. It also serves as the central point of contact at the national and international levels for all computer security incidents where at least one of the involved parties is based in Montenegro. CIRT works on incident resolution, response, and coordination, prepares security alerts and advice for users, and focuses on raising awareness and educating users.

The **Ministry of Defense (MoD)** and the Armed Forces of Montenegro are fully responsible for the cyberspace created

⁵ The total number of polling locations at the parliamentary elections was 1058.

within the MoD and cooperate with the national CIRT and MPA in Montenegro's cyberspace protection. After joining NATO in 2017, the Ministry of Defense and the Armed Forces of Montenegro have made significant efforts to enhance information security, particularly in the field of cyber defense, in line with the national and strategic objectives of NATO. In this context, changes have been made to the military and ministry organizational structures that clearly recognize the need to strengthen cyber capabilities in the defense arena.

The **National Security Agency (NSA)** is recognized in strategic documents as one of the key institutions responsible for cybersecurity in Montenegro, in line with its primary focus on protecting national interests and security. The laws regulating the work of the NSA define the agency's competencies, which primarily involve collecting and processing data of national security significance, as well as its position in counterintelligence activities and the protection of essential facilities and individuals. The NSA is central to exchanging classified information with partner intelligence-security systems and agencies, possesses advanced forensic tools, and can analyze sophisticated malicious programs.

The **Information Security Council of Montenegro** was formally set up on August 1, 2017, thus providing a national parent organization to advise the Government of Montenegro on all essential issues in this field.

The law establishes the Council as a multi-sector government body. Despite primarily including public institutions only, the Council is tasked with strengthening cooperation with the private sector and serving as a framework for establishing a permanent collaboration between the public and private sectors. The Council is focused on developing and strengthening cooperation with critical information infrastructure (i.e., internet service providers, the banking sector, and electric companies).

Cybersecurity Legal Framework

The **election-related acts** (the Law on the Election of Councilors and Members of Parliament, the Law on the Election of the President of Montenegro, and the Law on Voter List) do not contain specific cybersecurity or data protection provisions and rely on the general legal framework.

The legal framework for cybersecurity and data protection in Montenegro is governed by the **Law on Information Security** (first adopted in 2010, but a substantial revision of the law is planned in 2023) and the **Regulation on Information Security Measures**. As society becomes more digitally managed, there has been a significant increase in cyberattacks, underscoring the necessity for the robust protection of critical infrastructures and decisive steps in cybersecurity. This also includes bolstering national cyber defense capabilities and responses to cybercrime, both of which also resonate in the context of elections. These also regulate the protection of personal data and the obligations of providers of electronic communication services regarding data retention and cooperation with competent authorities.

Montenegro has recently implemented a series of strategic frameworks and organizational constructs about cybersecurity. The **National Security Strategy** and the **Defense Strategy of Montenegro**, which cover cybersecurity, were instituted in February 2020. Moreover, a contemporary Cybersecurity Strategy was set in motion from 2022 to 2026, succeeding two antecedent strategies from 2013 to 2017 and 2018 to 2021, respectively.

The information security legislation has been harmonized with the EU acquis. In addition, in 2016, the Law on Amendments to the Law on Information Security was adopted, providing for two key activities: the formation of the Information Security Council and the protection of critical information

infrastructure, which are in line with the NIS Directive (2016/1148)⁸. Additionally, amendments to the Law on Information Security, based on the Cyber Security Strategy 2013–2017, were adopted in 2016. Critical information infrastructure has been defined, and based on these amendments, eight critical sectors were identified. However, election infrastructure is not deemed part of the critical infrastructure in Montenegro.

The **Cybersecurity Strategy of Montenegro 2022–2026** represents an interdepartmental document that pertains to a five-year strategic period and is aimed at enhancing overall capacities (legislative, operational, human, financial, and technical) for an adequate response to the challenges and threats emerging from cyberspace within and outside of Montenegro.

The strategy aims to create a protected environment. The goal is that citizens, critical infrastructure operators, the economy, and public administration in Montenegro are protected to the greatest possible extent from the negative aspects of cyber threats and crime. This will be achieved through continuous education on the safe usage of information and communication technologies in everyday life and business, sharing know-how with national, regional, and international partners, and implementing measures for protecting critical information infrastructure. The strategy includes, among other things, activities related to harmonizing the legislative framework with the European Union's General Data Protection Regulation (GDPR) and establishing critical information infrastructure protection.

4. Assessment of the Election Management ICT Infrastructure

Context of the Election Management ICT Infrastructure

A 2022 digital maturity assessment commissioned by the European Bank for Reconstruction and Development, conducted by the e-Governance Academy, found Montenegro to only have a “basic” level of digital maturity in seven categories, including “financing digitalization, level of digital skill, and access to services.” The same assessment found that the right conditions had been generated for the purposes of digitalization, but implementation fell short. These conditions included “political will and support, the legal framework, digital infrastructure and interoperability, digital identity/signature and security.”⁶

Montenegro ranks 87th in the world according to the Global Cybersecurity Index and 97th in the National Cyber Security Index.⁷ According to an OSCE survey on public perceptions and confidence in election management bodies in Montenegro (2021), a high percentage of citizens (80.2%) believed that election fraud (all irregularities that

may negatively affect the election result) is a problem in implementing election processes in Montenegro.⁸ The crisis of trust in the electoral processes, which has mostly stayed the same since the survey, could be addressed with IT solutions, increasing transparency, and providing a way for trustworthy official information. For example, slowness and inconsistency in the publication of official election results require citizens to rely on civil society organizations for results.

Montenegro has been increasingly targeted by cyberattacks in recent years.

Montenegro has been increasingly targeted by cyberattacks in recent years. In parallel with the accession negotiations and later during Montenegro’s entry into NATO, the IT infrastructure of state bodies was explicitly targeted by cyberattacks. The types, intensity, and scope of these attacks ranged from the least technically demanding to the most sophisticated. October 16, 2016, the day of parliamentary elections, witnessed large-scale DDoS attacks launched against

6 EU Cyber Direct. Montenegro. <https://eucyber-direct.eu/atlas/country/montenegro>

7 Global Cybersecurity Index. Montenegro <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E and National Cyber Security Index. Montenegro. https://ncsi.ega.ee/country/me/>

8 OSCE. Survey on public perceptions and confidence in election management bodies in Montenegro. Nov 26, 2021, p. 3: <https://www.osce.org/mission-to-montenegro/505747>

state web pages and IT infrastructure, as well as the websites of pro-NATO and pro-EU political parties, civil society web pages, and electoral monitors. Several days later, a phishing attack was launched against the Parliament of Montenegro.

So far, the public has not been notified of any successful cyberattacks during the elections in 2023.

The trend continued well into 2017, with an even larger DDoS attack recorded in February, compromising government and state institutions' web pages and several pro-government media. In parallel, the MoD reported being targeted by spear-phishing attacks. In June of the same year, further cycles of similar attacks were reported in light of Montenegro's official accession to NATO. Anticipating new cyberattacks during the parliamentary elections of 2020, NATO deployed a counter-hybrid team to Montenegro in late 2019 and early 2020 to strengthen the country's capacities in deterring hybrid threats.

None of the attacks detected until the attack conducted in August 2022 had consequences that would paralyze the operation of critical services. However, the latest attack in 2022 has significant implications. The target of the 2022 attack was the IT and communication infrastructure of state authorities. First, the most significant impact was dealt to the government domain, gov.me. The IT system of the Parliament of Montenegro was also a target of the attack. Almost all government services, including those aimed at citizens, became unavailable, which caused anxiety among the general public and prepared a suitable ground for spreading misinformation. There was also deep concern about the influence of external factors on the electoral process and fear of potential cyberattacks during the

presidential elections in March 2023. So far, the public has not been notified of any successful cyberattacks during the elections in 2023.⁹

The draft of the law on information security (March 2023) defines cyber threat as "any possible circumstance, event or action that could damage, disrupt or otherwise negatively impact data and network and information systems, users of those systems, and other authorities and persons" and a serious cyber threat as a "cyber threat which, based on its technical characteristics, can be assumed to have a serious impact on the network and information systems of an entity or user of the entity's services by causing significant material or non-material damage."¹⁰ The information technology used for elections is a distinct example of a system that, when targeted successfully, can cause severe damage to the reliability of the authorities involved as well as the state.

The information technology used for elections is a distinct example of a system that, when targeted successfully, can cause severe damage to the reliability of the authorities involved as well as the state.

-
- 9 Report on Preliminary Findings and Conclusions. Podgorica, March 20, 2023. Citizen Election Monitoring. Presidential Elections Montenegro 2023, p. 3. <https://cemi.org.me/storage/uploads/SrGrpOWJRUvB8H5m7ccroLyomtySx5pqYQLS7Gk.pdf>
 - 10 Zakon o informacionoj bezbjednosti (law on information security [Montenegro]). Draft (March 2023). Article 5.

The critical components in the election ICT infrastructure in Montenegro are:



Voter register database



Web page for voter data checking



Web page for verification of signatures in support of election lists



Web page for voting results and election information



Voter identification devices (hardware + software)

Threats and Security Measures for the Voter Register

The **Voter Register (VR)** is a permanent database maintained by the MoI. The data is updated automatically with information extracted from citizenship, residence, birth, and death registers. The VR is checked for duplicates in advance of each election.

Before elections, excerpts are made of the VR for each polling station. All the passages containing VR data for each polling station are encrypted and transferred to voter identification devices. The data can only be decrypted by special eTokens given to the polling station director and deputy, and the decryption occurs on the morning of election day. The eTokens are paired with voter identification devices, and these devices cannot work without them.

The MoI is responsible for printing out paper voter lists for all polling stations. Voter lists are used if voter identification devices are out of service for more than a period of one hour.

Previously, concerns have been raised about the accuracy of VR data, questioning the accuracy of permanent residence data, possible duplicated entries, the entries of deceased persons, and the number of voters compared to census data. Further, some

stakeholders stated that controversies related to allegations of a high number of voters fictitiously changing their permanent residence shortly before the local elections further reduced trust in the accuracy of the VR.¹¹

According to the law, parliamentary parties and the SEC have permanent online access to the VR. Accredited observer organizations and authorized representatives of contestants have the right to inspect the VR online in the pre-election period upon request. They are granted full access to the VR data, including filtering it by any parameter; however, making copies of any data is forbidden. The parliamentary parties are also granted this access outside of the election period. While this access allows for a meaningful verification of individual entries, some stakeholders have criticized the legal provisions on data protection prohibiting the extraction and printing of the data stored in the VR.¹²

Voters may verify their personal data in the VR through a dedicated website (biraci.me) or in person at local MoI offices and can

11 OSCE. Needs Assessment Mission Report: Montenegro. Presidential Election, March 19, 2023, p. 7. <https://www.osce.org/odihr/elections/montenegro/537023>

12 Montenegro Parliamentary Elections, August 30, 2020, ODIHR Limited Election Observation Mission Final Report, p. 9 <https://www.osce.org/odihr/elections/montenegro/473532>

request corrections or amendments. Although the VR remains one of the key elements in the voting process, other databases – the births and deaths registry, citizenship registry, and residence registry – are used to compile the VR. The signature database used by SEC to identify voter signatures given in support of a candidate list and the fingerprints database, used by MoI for deduplicating voters' fingerprints and, therefore, for checking voter data for duplicates on the VR, are also indirectly part of the election process and the same protection measures should apply to these databases.

VR data is the primary source for populating voter identification devices and printing voter lists. Each computer used for adding, changing, or deleting data from the VR can threaten the integrity of the database if infected by malware or used by attackers to access the VR. To ensure the integrity of the VR, all activities concerning the maintenance of the VR and making any changes to it or accessing it should have clear and appropriate policies in place. As the landscape of cyber risks is rapidly changing, the VR should have regular security audits conducted by certified officials and tests against possible cyberattacks.

Main Threats

The **main threats** to these databases are:

- unauthorized modifications of the voter data, increasing mistrust;
- blocks and delays in VR compilation, causing stalls in data transfers from the VR to voter identification devices and voter list printing;
- data breaches that cause sensitive or personal information to be collected by malicious actors, as many people have access to all VR data.

Security Measures

The following **security measures** have already been introduced:

- the VR can only be accessed through the government network;
- voter data encrypted for transfer;
- the proposed amendment of the law on information security prescribing information security measures for network and information systems;
- a national framework for network and information system security;
- a process for managing cyber-security, supervision over key entities, and other matters of importance for achieving a high level of information security;
- regulations governing personal data protection and information security are applied to collecting, processing, and using voter data.

Threats and Security Measures for Election-Related Web Pages

There are several web pages displaying election-related information – the web page for voters to check the accuracy of their data, <http://biraci.me>; a page for verifying signatures given in support of the candidate list, <https://provjeripotpis.me/>; and a government web page with information about polling stations, election proceedings, and election results, <https://dik.co.me/>.

Voters can verify the accuracy of their personal data for a certain period before elections from a website or in person at local offices of the Ministry of Interior and request amendments, if necessary. The lists are closed to any changes ten days before election day.

The **biraci.me** page requests a voter's ID card or passport number as input, has a reCAPTCHA verification section, and returns information about the voter's polling station (number, name, description, and address) as well as the voter's initials, address, and municipality of residence. Voters can request a change of residence address, which will be submitted to the regional unit/branch for administrative internal affairs if the data in the database is incorrect. The page states, "Any abuse of this service is punishable by law," but no terms of service are provided. The Ministry of Interior is responsible for maintaining and protecting the biraci.me website.

The SEC-owned provjeripotpis.me web page for verifying signatures of support for the candidate list requires an ID code and an ID card or passport number as input. If the voter's data is found in the database of voters who have provided a signature of support, which has been processed by authorized personnel during the verification of support signatures, the voter's data and the name of the electoral list or the candidate they have supported are displayed on the screen. Signatures are not displayed on the web page. The SEC, following the instruction on the method of verifying signatures of support for the electoral list for the election of members of parliament and candidates for the President of Montenegro, only enters a portion of support signatures to this database of the candidate list, as a certain number (1.5 percent of the total number of voters¹³) of valid signatures are sufficient to determine support for a candidate list.

The law does not prescribe detailed rules on signature verification. There have been complaints by voters who alleged the misuse

of their signatures¹⁴, and some stakeholders noted in 2023 that the signature collection process could be open to abuse.¹⁵ In February 2023, three weeks after the inception of the nomination period and after the confirmed registration of one of the candidates, the SEC adopted an instruction on signature verification, partly regulating the process. The SEC verifies whether the data of voters who provided signatures correspond to their data in the VR. The SEC verifies the signatures until it reaches the legally required number of valid signatures, and the rest are not checked. If the SEC identifies that a voter has already supported a previously registered candidate, only the signature for the first verified candidate is deemed valid.

The SEC web page for general election information dik.co.me is used, among other materials, to publish preliminary voting results. Polling stations have 12 hours from closing to deliver their results to the MECs; MECs have an additional 12 hours to establish, publish and submit the tabulated results to the SEC; the SEC has an extra 12 hours to establish and publish the preliminary results on their web page (in practice 48 hours after the elections).

The results are not published in a unified manner; for example, some MECs published disaggregated data in scanned MS Excel files or in scanned individual polling station protocols for the second round of the presidential elections in 2023. Moreover, some

13 OSCE. Montenegro Presidential Election, 19 March 2023: Interim Report 8 February – March 1, 2023, p. 6. <https://www.osce.org/odihr/elections/montenegro/538389>

14 OSCE. Limited Election Observation Mission. Montenegro, Parliamentary elections, August 30, 2020: Interim report, August 5–15, 2020, August 19, 2020, p. 9. (<https://www.osce.org/odihr/elections/montenegro/460846>) and OSCE. Montenegro, Parliamentary elections, August 30, 2020: Statement of Preliminary Findings and Conclusions, p. 8. <https://www.osce.org/odihr/elections/montenegro/462016>

15 OSCE. Montenegro, Early Parliamentary Elections, June 11, 2023: Statement of Preliminary Findings and Conclusions, p. 7. <https://www.osce.org/odihr/elections/montenegro/545938>

scanned files were illegible.¹⁶ According to the SEC, phone or email is primarily used for data exchange (results, voter turnout statistics, and ballot statistics), and more secure communication channels are not provided.

Potential Threats

As all of the web pages mentioned above are part of election processes, the **potential threats** are as follows:

- denial of service, as some election procedures are time critical, the web page being unavailable could jeopardize elections in general;
- skewed or false data on web pages, causing mistrust and complaints;
- hijacking, a malicious actor could display an alternative message;
- data phishing, names, ID codes, and ID card or passport numbers could be collected by attackers.

Security Measures

The following security measures have been taken to protect some election-related web pages from cyberattacks. However, these are not implemented equally for all of the associated pages.

- the web page for checking voter data is only accessible from Montenegro DNS servers;
- the authentication methods for managing web pages have been improved and require strong authentication;
- SSL/TLS encryption is used;
- firewall protection is enabled;
- activity logging is engaged.

Threats and Security Measures for Voter Identification Devices

Devices for electronic voter identification were procured in 2015 and introduced in elections in 2016. The devices are described in the law on the election of councilors and members of parliament as a compact hardware and software unit composed of an electronic reader of a machine-readable record from an ID card or passport, a computer that stores a copy of the closed voter list for a specific polling station, including the last photograph of the voter from the register of ID cards or passports, and a printer that prints a confirmation of successful voter identification.

These devices contain information about the polling station where they are activated, the date, time, and a copy of the voter list for that polling station and the ongoing elections. Each device contains only statistical data on the turnout for the polling station where the device is located. Voter data appears when an ID card or passport is swiped through the device's reader, provided the voter is registered at that polling station. The devices for electronic voter identification are owned and controlled by the MoI. They are not connected to the internet, and the devices are not interconnected. The data stored in them are supposed to be erased within 30 days from the day the final election results are announced.

Threats

The **threats** to voter identification devices are:

- unavailability: the devices depend on a direct power supply and have no independent power source;
- distorted data: a device displaying only partial or false data could skew the election process.

16 OSCE. Montenegro, Presidential Election, Second Round, April 2, 2023: Statement of Preliminary Findings and Conclusions, p. 4. <https://www.osce.org/odihr/elections/montenegro/540584>

As stated by ODIHR observers in April 2023,¹⁷ the devices mostly work well, with only some being unavailable during election day. The polling stations are equipped with paper lists, so the voting process is not interrupted if the device is out of service. Still, as a part of election technology, the cybersecurity of the devices needs auditing, as no software or hardware audits (besides some functionality checks before elections) have been conducted since the introduction of the devices in 2016.

17 OSCE. Montenegro, Presidential Election, Second Round, April 2, 2023: Statement of Preliminary Findings and Conclusions, p. 10. <https://www.osce.org/odihr/elections/montenegro/540584>

5. Risks and Recommendations

In summary, the ICT technology used for elections in Montenegro is **fragmented** and various components have **different cybersecurity approaches and measures**. The main risks derive from a lack of unified rules applicable to all the components and stakeholders. Undoubtedly, some features in the larger ecosystem of election ICT infrastructure have been introduced with stringent security measures. Still, similar rules must be expanded to other components to gain a more significant effect.

The introduction of any completely new technological solutions would need to be defined in the electoral law, which requires, in the Montenegrin case, a more considerable political consensus of a two-thirds majority. However, more technical regulations and policies that determine the rules, i.e., database access, networks, and web page handling, could be introduced more rapidly. The following list arranges risks by criticality and includes recommendations to mitigate them.

High Criticality Risks



I Risk: IT infrastructure lacks precise rules for guaranteeing cybersecurity that should be implemented thoroughly and systematically for all election-related systems and components. Regular auditing, testing, and plans for improvement are not specified in regulations and policies.

Recommendations:

- 1) **Regular security audits and tests:** These must be regularly conducted by a cybersecurity task force or third-party companies. Such audits and tests can reveal serious security vulnerabilities and offer detailed improvement instructions. The process should be scheduled with the consideration that vulnerability fixes must be applied in a timely manner before elections, so any fixes and further testing would not interrupt the election process.
- 2) **A dedicated task force with a clear and transparent chain of command should be set up to encounter possible incidents quickly:** The main aim of a cyberattack may be to cause mayhem and confusion. As the initial phase of detecting a cyberattack includes investigating its scale and severity, there should be a specific plan for how to act, who is informed, who issues the essential fixes, and how information about the incident is gathered and processed later to prepare action plans for improvement.
- 3) **Uniform cybersecurity policies and procedures should be in place (e.g., for networks, computers):** Security policy for all officials, institutions, and third-party companies with access to the VR or web pages and maintaining any election-related databases should set the rules. For example, what networks are allowed to be used for accessing the database, how computers are configured, how

passwords are used and stored, and what physical security measures are implemented. Policies should be updated regularly to include new rules or considerations, and old ones should be discarded.

- 4) **Limited and controlled user access and a clear user policy in place:** All access to the Voter Registry database or web pages should be controlled with user rights, giving each user the minimum rights necessary for their duties.
- 5) **Logged and monitored user activity:** Logging and monitoring user activity in election-related databases and web pages displaying voting results should be used as a mitigation tool. Any suspicious activity should create an alert and be investigated immediately, shortening the time the database or web page is vulnerable.



II Risk: Outdated software causes systems and web pages to be vulnerable to malicious activities.

Recommendations:

- 1) **Regular software updates and server patching should be the norm:** Outdated software contains vulnerabilities that enable malware planting in systems. Updates are essential to improve software and server performance and to keep both functioning reliably. Security policies should describe regularity to ensure sufficient funding is provided on time.
- 2) **Using licensed or controlled open-source software and ensuring timely renewals:** Database software or other solutions used to maintain databases and software for managing web pages should be licensed and renewed on time. Alternatively, consider using open-source software by respected and trusted creators.



III Risk: No sufficiently detailed risk evaluation or crisis plans.

Recommendations:

- 1) **Risk evaluation and compulsory incident notification:** Creating a detailed risk evaluation document for all possible factors and prioritizations provides preparation for individual risks and combined attacks. All stakeholders should have a compulsory incident notification policy, even if the incidents do not immediately affect the election process.
- 2) **Crisis management plans, response plans, and communication plans:** These help to calm the situation if an incident has happened and to provide efficient risk management mechanisms. This is especially important as elections are time-critical, and there is no time for excessive research on the origins of a problem, so quick workaround guides should be in place. Disaster recovery plans and checks should be in place in case of an attack. These must include regular backups and rules for storing/retrieving backups (cloud services or offline solutions). No plan is effective without the appropriate awareness of user expectations; therefore, all crisis management measures have to contain communication and awareness-raising elements.
- 3) **Guidelines, drills, and simulations for cyber hygiene and presenting relevant good practices:** These are essential for forming safe cyber habits for existing technology. This is also important for possible future developments, as these will expand the user base, and their awareness could be enhanced earlier.



IV Risk: A lack of security rules and policies for voter information and web page management can compromise sensitive voter data.

Recommendations:

- 1) **Website activity logging and monitoring:** Election-related websites that display any voter information can be a threat to voter identity theft and the infringement of privacy. Various network security tools – for example, an Intrusion Protection System, an Intrusion Detection System, or firewalls – monitor the network and detect malicious activity or anomalies in network traffic and can block or prevent some attacks early. Logging website traffic can be a valuable tool to investigate when and from what IP address the data was accessed and if any incident should occur. In case some form of logging has already been introduced, the logs from previous elections could be used to define what is typical and expected traffic and, therefore, help to define abnormal behavior that should alert the authorities.
- 2) **Data validation and encryption:** Election-related websites have text fields where users can enter some strings to search for information. These data fields could be used to inject malicious scripts that could disable the web page as cross-site scripting (XSS). To prevent that, form validation on the client or server side should be used to validate the syntax of the entered text. All websites processing voter data should be encrypted using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) certificates.



V Risk: A lack of official vote tabulation and reporting system and inconsistencies in displayed results could erode trust in official results.

Recommendations:

Unified structure for vote tabulation and displaying results using open data:

Preliminary voting results are mainly presented by civil society organizations, not official institutions. The official election website should be the primary source for unified, reliable, and comparable voting data and calculations to build and secure trust in government authorities. This requires a dedicated secure digital environment where polling stations or municipalities can enter the preliminary voting results, which could be displayed on the official SEC website. Additionally, to further increase public trust in vote tabulation, all election-related data should be downloadable in a machine-readable format, so all interested parties can recalculate the preliminary results if needed. Over time, new modules could be introduced to the tabulation system to gather all election processes – such as voter data checks, signature verification, and candidate lists – under one centrally managed unified and secured system.

Medium Criticality Risks




I Risk: A lack of broad-based cybersecurity and cyber hygiene training.

Recommendations:

- 1) **Enhance the overall awareness of cyber threats:** Educating and training election staff about various cyber threats will improve the safety of election web pages as well as cyber hygiene habits in general. The more trained eyes there are monitoring the web pages – that is, technical and non-technical staff – the quicker the detection of any anomalies


in data or web page performance. There should be clear, real-life examples of what a hijacked or malware-infected web page looks like and how it behaves. In the future, if the aim is to increase technology usage during elections, more proper cyber safety training will become critical, as cyber criminals primarily target human errors in technology users.

- 2) **Regular cybersecurity awareness training for personnel using databases:** Unfortunately, human mistakes are the major contributing factors to data breaches. Any computer used to access a database is a possible threat to integrity. Cybersecurity training with real-life examples helps employees to recognize various threats and attempts to gain unlawful access. There should also be a step-by-step action plan if something suspicious happens, as not all cyberattacks are visible immediately. All new employees should have cybersecurity training as a part of the onboarding process.

 **II Risk:** Physical security measures of voter identification devices are unclear between elections.

Recommendations:

Physical security of the devices between elections has to be regulated in more detail: The physical security and maintenance of the devices between elections have to be a part of the broader security policy to guarantee the appropriate conditions for keeping these devices, as well as proper handling and protection to avoid any damage.

 **III Risk:** There is a deficit of specialized IT personnel in election management.

Recommendations:

Creating a community of all election stakeholders: The exchange of information about any threats, incidents, or attacks can be highly beneficial to all institutions. Such exchanges provide an opportunity to recognize a pattern in criminal activity and, as a result, be better prepared for attacks, raise awareness of the broader threat landscape, and cooperate in opposing criminals. As it might be challenging to hire dedicated IT personnel for the public sector, forming an (unofficial) cooperation network by engaging experts from the public sector, private sector, and academia in sharing expertise and experience between stakeholders would be beneficial. Additionally, this would allow different competencies to be aligned and avoid duplication. Also, such cooperation allows for better planning to ensure that available funds and financial resources are used as efficiently as possible.

Annex

List of consulted stakeholders

- Prof. Dr. Ramo Sendelj – Research Chair in Cyber Security, University of Donja Gorica, Institute of Modern Technology Montenegro (May 25, 2023)
- Ms. Ana Nenezić – Executive director of CeMI (Centre for Monitoring and Research) Montenegro (May 16, 2023)
- Ministry of Interior election ICT delegation led by Mr. Igor Pekic – Advisor to the Ministry (May 10, 2023)
- Ms. Milijana Radulovic – Consultant (ICT) of the State Election Commission of Montenegro (April 28, 2023)
- Ministry of Interior election ICT delegation led by Mr. Igor Pekic – Advisor to the Ministry (April 28, 2023)
- Ministry of Foreign Affairs delegation led by Mr. Lazar Popovic – Head of the Information Systems Management Service (April 27, 2023)
- Ministry of Public Administration delegation led by Mr. Dusan Polovic – Director General of Directorate for Infrastructure, Information Security, Digitalization, and e-services (April 27, 2023)



@ eGA

e-Governance Academy
Rotermanni 8, 10111 Tallinn
+372 663 1500 | info@ega.ee | ega.ee
Facebook, LinkedIn, Twitter: egovacademy

