POST-ELECTION ASSESSMENT OF THE CYBERSECURITY INFRASTRUCTURE AND INTERAGENCY COOPERATION IN UKRAINE WITH RELATED RECOMMENDATIONS

EU Project Countering Election-Related Cyber Threats and Disinformation Campaigns in Ukraine
This document has been prepared under the terms of the European Union funded project Countering Election-Related Cyber Threats and Disinformation Campaigns in Ukraine.

The content of this document is the sole responsibility of the consortium of the Estonian Center for Eastern Partnership and CybExer Technologies OÜ and can in no way be taken to reflect the views of the European Union.
# TABLE OF CONTENTS

1. EXECUTIVE SUMMARY  
2. METHODOLOGY  
3. BACKGROUND AND CONTEXT  
   3.1 WHY CARE - INCIDENTS AGAINST ELECTORAL IT INFRASTRUCTURE  
   3.2 UKRAINIAN ELECTION SYSTEM AND IT INFRASTRUCTURE  
   3.3 LEGAL FRAMEWORK  
   3.4 KEY PLAYERS IN NATIONAL CYBERSECURITY  
4. ASSESSMENT OF THE IT INFRASTRUCTURE  
   4.1 THREATS TO THE STATE VOTER REGISTER  
   4.2 PROTECTION MEASURES FOR THE STATE VOTER REGISTER  
   4.3 THREATS TO VYBORY  
   4.4 PROTECTION MEASURES FOR VYBORY  
   4.5 TRAININGS AND EXERCISES  
   4.6 RISKS AND RECOMMENDATIONS  
5. ASSESSMENT OF INTERAGENCY COOPERATION  
   5.1 COOPERATION BEFORE AND DURING THE 2019 ELECTION  
   5.2 RISKS AND RECOMMENDATIONS  
6. CONCLUSIONS  

Annex I - External resources on electoral cybersecurity  
Annex II - Competencies of the main national cybersecurity stakeholders
PREFACE

Within the framework of the project “Countering Elections-related Cyber Threats and Disinformation Campaigns in Ukraine”, the Delegation of the European Union to Ukraine (EUDEL) has contracted a consortium of the Estonian Center of Eastern Partnership and CybExer Technologies OÜ to improve the resilience of the Ukrainian electoral system to cyber threats and disinformation campaigns.

This report, conducted by CybExer Technologies OÜ, marks the completion of works of the post-election assessment and presents the final results of the analysis of cybersecurity procedures and interagency cooperation during the 2019 presidential elections in Ukraine.

The aim of the assessment was to evaluate the procedures and practical cooperation between Ukrainian agencies responsible for cybersecurity and for electoral administration: how did the management of the systems and the technologies used during the elections function, and how did various agencies work together during the elections to solve problems? The report provides practical recommendations on how to improve interagency cooperation, as well as the regulatory framework in order to protect the integrity of election results. The overall goal has been to strengthen Ukrainian resilience against cyber threats ahead of next elections.

The report will be presented to key Ukrainian cybersecurity stakeholders and the EUDEL. A draft of this report was discussed in a “Post-Election Assessment Verification Workshop” on June 10, 2019, in Kyiv with relevant interagency Ukrainian stakeholders. Their inputs, observations and suggestions guided the finalisation of this report.

LIST OF ACRONYMS

CEC - Central Election Committee of Ukraine (Центральна виборча комісія)
DEC - District Election Commission (Окружна виборча комісія)
EUDEL - Delegation of the European Union to Ukraine (Представництво Європейського Союзу в Україні)
IFES - International Foundation for Electoral Systems
NCCC - National Coordination Centre for Cybersecurity (Національний координаційний центр кібербезпеки)
NSDC - National Security and Defence Council of Ukraine (Рада національної безпеки і оборони України)
OSCE - Organization for Security and Co-operation in Europe
PEC - Precinct Election Commission (Дільнична виборча комісія)
RAB - Register Administration Bodies (Розпорядник Реєстру)
RMB - Register Maintenance Bodies (Органи ведення Реєстру)
SOC – Security Operations Centre
SSU - Security Service of Ukraine (Служби безпеки України)
SSSCP - State Service of Special Communications and Information Protection of Ukraine (Державна служба спеціального звʼязку та захисту інформації України)
SVR - State Voter Register (Державний реєстр виборців)
UK Aid - development fund managed for the UK government
USAID - United States Agency for International Development
1. EXECUTIVE SUMMARY

The report assesses the management of cybersecurity systems and the technologies used during the 2019 presidential elections in Ukraine, with a focus on interagency cooperation in guaranteeing the security of electoral IT systems and on the actual incident response during the elections. The report aims to support and inform electoral cybersecurity managers in Ukraine.

The 2019 presidential elections in Ukraine were an important test for Ukrainian democracy and the country’s ongoing reform efforts. The elections took place amidst a difficult political, economic and security environment and against the backdrop of ongoing challenges to Ukraine’s territorial integrity that started in 2014. In addition to more traditional military threats, Ukraine also suffered severe attacks on its electoral IT systems during the 2014 presidential elections: files necessary for vote tabulation were destroyed, core network nodes of the electoral IT system were disabled and disinformation campaigns were conducted. In the following years and in response to these attacks, the Central Election Committee (CEC), who is responsible for carrying out elections, began updating several parts of the electoral IT system. It segmented the office network and critical networks; installed a comprehensive network monitoring system with modern firewall, proxy, and SIEM; replaced outdated critical network equipment; and upgraded the system’s major hardware and software components.

Considering the improvements to the electoral IT systems in recent years and the inevitable developments in the nature of cyber threats, the report provides a fresh assessment of the cybersecurity of the Ukrainian electoral system that can inform future improvements of the IT systems. The report looks at the technical and operational sides of cybersecurity (e.g. legal framework, key stakeholders, cooperation mechanisms, technical set-up). The political aspects of cybersecurity are not analysed.

Based on the technical and operational analysis of cybersecurity, the report provides 12 risks and corresponding recommendations for the Ukrainian electoral IT system. The findings of the report suggest that the cooperation between principal institutions responsible for cybersecurity was effective and successful therefore, principles of cooperation should not be changed. The preparations for elections were well-planned and well-executed; information sharing between institutions was adequate. Every agency followed its respective scope of responsibility. These adequate safeguards did at the end of the day play a role in ensuring that despite around 9000 cases (including a relatively sophisticated malware by the hacker group Dragonfly) related to cybersecurity no major incidents took place before or during the elections.

However, there are significant gaps in a number of areas. For example, the legal framework does not fully support the security of elections – notably, the IT systems of the Central Election Committee are not listed as critical infrastructure and, therefore, do not receive the necessary attention from stakeholders legally responsible for national cybersecurity and is financially underserved. But perhaps the key weakness of the current management of cybersecurity is the lack of technical personnel within the CEC where only a few technicians cover elections-related systems across the whole country.

While most risks are considered to be of medium or low criticality, the risk of outdated security measures that do not correspond to relevant latest threats and risk assessments is seen as of high criticality. Thus, the report recommends that for electoral IT systems, risk analysis and vulnerability assessments should be regularly conducted and updated, as the landscape of cyber threats is rapidly changing and new vulnerabilities are constantly discovered. Risk analysis should be followed by implementing timely mitigating measures to protect IT systems from cyber threats. Below, the top three risks and recommendations for both IT infrastructure and interagency cooperation are presented. Complete tables are provided in the main body of the report.

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk Description</th>
<th>Recommendation</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outdated security measures do not correspond to relevant latest threats and risk assessments.</td>
<td>To regularly conduct risk analysis and vulnerability assessment of electoral IT systems. The landscape of cyber threats is rapidly changing and new vulnerabilities are constantly discovered – this calls for regular and updated risk assessments. Risk analysis should be followed by implementing timely mitigating measures to protect IT systems from cyber threats. Analysis of previous incidents should be considered a valuable source of information for updating risk analysis.</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Outdated physical security measures do not correspond to relevant latest threats and risk assessment.</td>
<td>To assess the physical risks to infrastructure (including workstations). Considering that a large number of District Election Commissions around the country are using Vybory and around 680 Register Maintenance Bodies work on the State Voter Register (SVR), physical risks are unquestionable.</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Assigning too low of a priority to the protection of electoral systems that may result in insufficient resources to identify, analyse and recover from cyber incidents.</td>
<td>To include the CEC’s IT systems Vybory and SVR in the official list of the state’s critical infrastructure which is currently in preparation by the SSSCIP and due to be passed by the government. This would prioritise the protection of the CEC’s IT systems and provide additional resources for the CEC.</td>
<td>High</td>
</tr>
</tbody>
</table>
Table 2. Top 3 risks and recommendations for interagency cooperation

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk Description</th>
<th>Recommendation</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unclear responsibilities for the protection of electoral systems.</td>
<td>To document and formalise the ad hoc cooperation measures used by the CEC in its cooperation with other agencies during the 2019 presidential elections. The formalised cooperation regulations should identify the responsibilities of various stakeholders tasked with protecting and monitoring electoral IT systems during the election period. However, the details of the cooperation procedures should not be fixed too rigidly at a legal level; some flexibility is necessary in different situations and regulations should support a bottom-up approach as well.</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Ineffective protection measures of electoral systems due to unclear criteria for the selection of experts</td>
<td>To stipulate in the above-mentioned cooperation regulations the specific functions and roles for the experts from other relevant authorities who are needed to protect the Vybory and SVR systems. Based on the respective roles, the relevant authorities could have specific criteria for selecting experts to the working groups at the DEC level or to the operational centre. The resolution should also provide guidelines for how the experts are to analyse and report technical and organisational measures applied to electoral IT systems.</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Developing or maintaining electoral systems without considering all important security requirements.</td>
<td>To ensure that agreements with third parties involved in development or maintenance of electoral IT systems (i.e., system developers, hosts, support service providers) cover all relevant security requirements. Care should be taken to include all identified risks in these agreements.</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Building resilience against cyber threats is a constant battle. The Ukrainian electoral organisations have shown so far the required determination – it is of utmost importance that the relative success of the 2019 presidential elections will not create complacency but rather serve as a motivational force to carry out further improvements of the cybersecurity of the electoral system.

2. METHODOLOGY

The data for this report was collected via interviews with key stakeholders, a study of Ukrainian legislation on cybersecurity and elections, observation of electoral procedures in Ukraine, monitoring of the media, and desk research.

The semi-structured interviews were conducted with key experts from the Central Election Committee (CEC), the Security Service of Ukraine (SSU), the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), and the National Security and Defence Council (NSDC). A questionnaire to support the interviews was drafted based on public data, including legal acts, websites of the Organization for Security and Co-operation, the CEC, the SSU, the SSSCIP and other relevant publications.

A member of the project team was registered by the CEC as an official observer of elections and followed the voting procedures and tabulation of results during the first round of the 2019 presidential election. Further input for the assessment was gained through a technical cybersecurity exercise conducted in Kyiv by CybExer Technologies on 3-7 March 2019 and through the preparation for the strategic-level table-top cyber exercise “Elections Cyber-Threat Modelling Workshop” on 21 May 2019.

3. BACKGROUND AND CONTEXT

3.1 WHY CARE - INCIDENTS AGAINST ELECTORAL IT INFRASTRUCTURE

The 2019 presidential election in Ukraine were an important test for Ukrainian democracy and the country’s ongoing reform efforts. The election took place amidst a difficult political, economic and security environment and against the backdrop of ongoing challenges to Ukraine’s territorial integrity that started in 2014.

Five years ago, Ukrainian electoral IT systems were the target of numerous attacks. During the 2014 presidential election, hackers infiltrated workstations and destroyed various files, including those necessary for vote tabulation. The CEC is the key node in Ukrainian elections as it is the institution responsible for the organisation of elections. On 21 May 2014, hacktivist group CyberBerkut disabled the core CEC network nodes and numerous components of the election system. For nearly 20 hours, the Vybory system, which is one of the two central IT systems for elections and which displays real-time updates in the vote count, did not function properly.¹ If the CEC’s network had not been restored by 25 May, the country would have

been unable to follow the vote count in real-time. On the election day of 25 May 2014, twelve minutes before polling closed, attackers posted a picture of Dmitry Yarosh, the former leader of the Right Sector, a right-wing political party, on the CEC website, incorrectly claiming that he had won the election. Beyond disabling the site and successfully displaying incorrect election results, CERT-UA discovered advanced cyber espionage malware in the CEC network. However, this attack could not have had an effect on the outcome of the election because all votes are manually verified. Nevertheless, the attack was well-planned, highly targeted, and had some (albeit limited) real-world impact.

According to OSCE observers, problems with the Vybory system in 2014 caused a major disruption of the receipt and processing of election material, prevented many district election commissions (DECs) from transmitting election results to the CEC, and delayed the CEC’s announcement of preliminary results. Nonetheless, the CEC started posting detailed preliminary results by polling stations on its website late on election night in 2014. All DECs submitted their tabulation protocols to the CEC well within a five-day deadline.

After the 2014 incidents, the CEC aimed to improve its cybersecurity principles on several occasions. It segmented the office network and critical networks; installed a comprehensive network monitoring system with modern firewall, proxy, and SIEM; replaced outdated critical network equipment; and upgraded the system’s major hardware and software components.

While the 2019 presidential election occurred securely and were not derailed, there were nevertheless some serious attempts to compromise the election through attacks on the ICT infrastructure. There were altogether about 9000 cases related to cybersecurity. Most of these cases involved scamming, DDoS attacks against the CEC’s web server; and attempts to penetrate the CEC network or web server. Moreover, other Ukrainian public authorities faced spear-phishing attempts with the aim to harm the electoral system.

During the pre-election period and on election days, the CEC gathered information about incidents (e.g. network scanning, internal attacks) as part of the monitoring process. According to CEC, their SIEM (security information and event management) and monitoring systems were able to register and block all malicious events. There were no disruptive availability incidents discovered regarding the Vybory system – it was up and running and monitored 24/7. As there were mirror sites from which to display Vybory results, unresponsiveness was not an issue.

The mirror sites belonged to the CEC and to the State Service of Special Communications and Information Protection (SSSCIP), which is the technical security and intelligence service under the control of the President of Ukraine and takes care of the technical protection of state information resources and information in cyberspace. Observation results confirmed that the CEC’s official website remained available and was updated regularly.

However, four notable incidents did take place shortly before or during the 2019 presidential election.

Firstly, false media reports alleged that the State Voter Register (SVR) database had not been updated since 2015. The aim of this was to erode the trust in the security of the SVR system and thereby in the integrity of the voter lists. To encounter the disinformation attacks, the CEC made an official announcement in February 2019 and stated publicly that since 2015, had updated the data of over 10 million citizens of Ukraine. The CEC also published the official numbers of voters on its website in the “Statistics” section as a proof of the correct information.

Secondly, on 14 and 23 February 2019, attacks against servers maintaining the official website of the CEC were carried out with the aim to block the preparatory information about the upcoming election. Using vulnerabilities of Wordpress, attackers’ botnet generated constant queries (“http flood”) that complicated the operation of the information system and blocked the access of ordinary users. As a countermeasure, the CEC introduced changes in the access-rights to network equipment and set up real-time monitoring to stop the attack on the website. The operational task force consisting of employees of the main institutions responsible for national cybersecurity, including the Secret Service of Ukraine (SSU), the SSSCIP and Cyber Police Department of the National Police, conducted an analysis on the functioning of the information infrastructure of the CEC. They concluded that the additional measures that were introduced were effective in blocking outsider access to CEC systems on the evening of the election.

Thirdly, in March, before the election, a large amount of regular Ukrainian users/voters checked their status in the online register. In response, the SVR was not completely unresponsive, but was slow and did reject some connections.

Fourthly, shortly before the first round of the presidential election on 31 March, an attack against Vybory was discovered and localised. As it became clear from the interviews conducted for this assessment, confidential sources from Ukraine have attributed the attack to the Dragonfly hacker group, operated by the special services of the Russian Federation. The purpose of the


4 The information was shared by relevant authorities during the “Elections Cyber-Threat Modelling Workshop” held in Kiev by CybExer Technologies OU in May 21, 2019.


3.2 UKRAINIAN ELECTION SYSTEM AND IT INFRASTRUCTURE

The presidential election in Ukraine were scheduled for 31 March 2019. The president is elected for five years through a nationwide majoritarian system. As no candidate won an absolute majority of votes in the first round, a second round between the top two candidates was held three weeks later on 21 April 2019.

Presidential elections are run by the Central Election Commission (CEC) which oversees the District Election Commissions (DECs), the Precinct Election Commissions (PECs), and the diplomatic and consular representations. In 2019, the two rounds of the election were managed through a three-tiered administration comprising the CEC, 199 DECs, and close to 30,000 PECs. There were over 30 million voters registered for both rounds. All votes are cast on paper ballots in Ukraine. The tallies are then counted in district commissions and the paper protocols of tabulation are sent to the CEC.

It is important to note the process around appeals concerning the lawfulness of election procedures (cyber incidents may cause grounds for appeals which in turn delay and eventually obstruct the normal course of elections). The right to appeal decisions, actions or inactions of election commissions and other authorities is granted to all participants in the election process. They can submit their complaints and appeals to the commissions and the courts. Complaints regarding the technical side of elections may be filed following the standard procedure of complaints on decisions, actions or inactivity of election commissions and their members, the candidates, their trustees and political parties. The Law on Presidential Elections defines the timeframes of appeal and the form of complaints. Even if the right to appeal decisions, actions, or inactions of election commissions and other actors involved in the process is granted to all participants in the election process, the elections law still allows for the rejection of complaints based on minor deficiencies in format. This part of the law has been criticized in OSCE election mission reports.

Internally, the CEC has divided cybersecurity responsibilities between two areas. For the State Voter Register (SVR) that holds information on voters and which is controlled by the CEC, a specialised department for information security has been created. Other IT systems and networks of the CEC are managed by the CEC's general IT department. Despite administrative preparations, the CEC lacks specialised cybersecurity experts; its main function is to carry out elections.

---


---

8. Resolution of the Verkhovna Rada of Ukraine of November 26, 2018 N 2631-VIII. The official start of the electoral process was set to December 31, 2018 by the Resolution of the CEC of December 27, 2018 No 253. The registration of candidates was carried out in accordance with the Decree of the Central Election Commission No. 62 dated January 15, 2019

Activities related to the election process are mostly paper-based, but electronic systems facilitate the information flow that is critical for carrying out paper procedures. The two main IT systems used for organising presidential elections are (1) the State Voter Register and (2) the Vybory system which is used for main electoral procedures like formation of polling stations, tabulation and determination of voting results, etc. Both systems are managed by the CEC and the main functionality is described in the laws (Law on Presidential Election 1999, Law on State Voter Register 2001).

The State Voter Register (SVR) is a centralised system for voter registration. It is updated monthly and maintained continuously by 25 Registration Administration Bodies (RAB) and 680 Register Maintenance Bodies (RMB) operated by 2,350 employees of the CEC. Voter registration is passive and continuous and is based on the centralised SVR. Voter lists are extracted from the SVR and compiled separately for each polling station. Preliminary voter lists together with voter invitation cards are prepared by each RMB for polling stations no later than 16 days before the election day.

Only the RMBs can “read and write” the data within their districts, the CEC has the right to “read only” the data for the entire population. Based on the electronic database, RMBs prepare the physical lists of the voters and transfer those before elections to Precinct Electoral Commissions (PECs), bodies responsible for organising the elections at the district level. Important to note that although the information about the voters is available to the public on the CEC website, the database itself is operated as a separate “closed system”.

Before elections, every voter has the right to receive information about their or other person’s inclusion (or non-inclusion) in the SVR. The PECs post voter lists for public scrutiny the day after they receive them to allow voters to verify their records and request amendments if necessary. Additionally, before and during 2019 elections voters were able to check their records online using a service called the Voter’s Cabinet and request amendments to their records with the Register Maintenance Bodies at their current residence.

Political parties can obtain the digitally certified electronic copy of the SVR’s database and verify the completeness and authenticity of data. This procedure can be done once a year, but not later than 60 days before election day. The CEC provides a compact disc with the electronic database, and political parties can obtain the digitally certified electronic copy of the database and authenticate credentials in a sealed envelope. In case of detected inaccuracies, political parties may ask a specific Register Maintenance Body to correct the mistakes. Political parties are prohibited from making electronic copies of the database and procedural measures are taken to prevent it. The CEC issues a document certifying the return of an electronic copy. If a party does not comply with the requirements, it loses the right to further receive electronic copies of the database.

The law on the SVR sets criteria for information security, especially the reliability of the information. The Register contains voters’ personal data as well as the place and conditions of voting. The law prohibits unauthorised access to the SVR, abuse of personal data and software protection policies and unauthorised use (Art 33). Registry officials can be held responsible for failing to fulfil duties related to ensuring the security of database; abuse of procedures and access rules; untimely or deliberate entry of knowingly false information; and the destruction of records. The law includes procedures for appealing decisions and actions of the registry administrators (Art 24).

In cooperation with the State Service of Special Communications and Information Protection, the CEC protects the security of the hardware and software of the SVR, and defends the integrity of the information held within its database. Together, they implement a set of security measures in the process of storing, processing and transmitting the data by telecommunication channels. The CEC establishes procedures for accessing the data and addresses the personal responsibility of the system administrators.

On 28 November 2018, the CEC installed equipment and software provided by the OSCE Project Co-ordinator in Ukraine for ensuring comprehensive technical protection of the State Voter Register, as part of efforts aimed at enhancing the security of election administration systems from digital threats. The new software made it possible to identify threats, prevent intrusions and respond to a range of possible cyberattacks. Through such comprehensive solutions, the system is able to respond to threats and anomalies at various levels, from workstations, network, and servers, as well as to various kinds of threats such as antivirus, spam, external network attacks or intrusions. The purchase and delivery of equipment was financially supported by the Government of Norway and the United States Mission to the OSCE. 11

The new software made it possible to identify threats, prevent intrusions and respond to a range of possible cyberattacks. Through such comprehensive solutions, the system is able to respond to threats and anomalies at various levels, from workstations, network, and servers, as well as to various kinds of threats such as antivirus, spam, external network attacks or intrusions. The purchase and delivery of equipment was financially supported by the Government of Norway and the United States Mission to the OSCE. 11

Also, the International Foundation for Election Security (IFES) contributed with the technical devices (like firewall, proxy, and SIEM) used for monitoring and network protection and for controlling the activities in the endpoints of the SVR. The website of the SVR dev.gov.ua was modernised a few months before the 2019 presidential election. It was optimised for mobile devices and new electronic services, such as a search function for finding polling stations, or the addition of new modules such as “My elections” and “Feedback”.

The Vybory Information and Analytical System is the set of organisational procedures, software and hardware (operating systems, database management systems, information security systems and telecommunication services) that provide collection, processing, storing and publication of information on elections.

Availability of the Vybory system is critical on the election day and in the few days following the elections. Before the beginning of the voting, PECs inform the DEC about the number of registered voters. The DEC transmits the specified information and the CEC will promptly publish them on its official website. During the day, the turnout results will be published. After the end of the voting, the PECs provide the vote tally protocols to the DEC and the DEC provides preliminary information to the CEC.

The detailed procedures for the DEC on using the Vybory platform are defined in the 2014 Project Co-ordinator provides solutions to enhance protection of Ukraine’s State Voter Register from cyber threats, OSCE Press Release, 28 November 2018
CEC Resolution\textsuperscript{12}. In chronological order the Vybory system is used by DECs for the following tasks:

\begin{itemize}
  \item Formation of polling station commissions;
  \item Ensuring the transfer of ballot papers, ballot boxes and paper protocols;
  \item Registration of official observers from candidates, political parties and public organisations;
  \item Forwarding the operative information on election day about voters included in the voters’ list and about the voters receiving ballots at the polling station;
  \item Establishing the preliminary results of voting within the territorial election district and to monitor the progress and results of voting; and
  \item Provision of information to the CEC for its publication on the official website in cases stipulated by the law (including decisions about complaints).
\end{itemize}

The primary goal and therefore the main threat vector of the Vybory system is to present the preliminary results of the elections in the most accurate and quickest way possible and thereby ensure the publicity and openness of the electoral process.

In addition to promptly publishing information about the voting results, the system also collects information on violations of the electoral legislation and on cases related to process complaints. For example, the decision of the DEC regarding a complaint, promptly after its adoption, is sent to the CEC through the Vybory system. Vybory also contains of modules for the oversight of campaign financing and modules for the exchange of documents between the electoral committees on different level.

According to the CEC’s resolutions, all should appoint system administrators and engineers to manage the software and hardware of the Vybory platform. The system administrator in the DEC enters the operational information received from the (deputy) chairman of the DEC into the system’s database. The official source of information is on paper (voting protocols, DEC decision, etc.). The system administrator then forwards the scanned copies through Vybory. In case of inaccuracies or technical abnormalities, re-entering of the specified information is carried out.

In 2003, the CEC approved the concept of the Vybory system. According to the concept, the system should prevent loss of information and unauthorised interference, destruction, distortion, forgery, and copying of information. The basis of the system is the CEC’s corporate computer network segment which should ensure a single information space and authorised access and protect the system from unauthorised interference, destruction and distortion of information flow. The corporate network resources guarantee reliable communication and data exchange as well as integration with automated systems of other public authorities. The traffic is encrypted. The concept emphasises that considering the high importance of the system, it is necessary to provide a backup for the creation of a subsystem and to use backup channels of communication networks and data transmission.

In January 2019, the CEC purchased services for updating Vybory. The winner of the tender was the original developer of the system: Scientific Development Enterprise Medirent Ltd. The contract was fulfilled in cooperation with InfoSafe Ltd. who was responsible for cybersecurity in the recent update of the Vybory platform.\textsuperscript{13}

\section*{3.3 LEGAL FRAMEWORK}

The legal framework that supports the cybersecurity of elections is based on two laws, a strategy and a number of complementary laws and regulations. The initial basics for cybersecurity were laid down in 1994 by the Law on the Protection of Information in Information and Telecommunication Systems which remained the key legislation for years. However, since 2014 significant changes have been introduced. Firstly, in 2014 the above-mentioned law was thoroughly updated. In 2016, the first cybersecurity strategy was compiled and in 2018 a specific law on cybersecurity was passed. Below, an overview of those major legislative acts and official policies is provided.

\textbf{LAW ON THE BASIC PRINCIPLES OF CYBERSECURITY (2018)}

With the adoption of the Law on the Basic Principles of Cybersecurity, which came into force in May 2018, Ukraine has a leading legislative act that establishes a comprehensive governance system for ICT security. It defines key cybersecurity principles; objects of cybersecurity and defence; cybersecurity roles, responsibilities and tasks; principles for the protection of CIIs; and guidance for international co-operation. It is worth noting that the main electoral IT systems are not yet listed as objects of critical infrastructure.

According to the law, private companies and public institutions are obliged to inform CERT-UA of cybersecurity incidents. Public institutions must also send incident information to the Secret Service of Ukraine. In order to facilitate the process, CERT-UA has prepared a form for incident reporting. In the case of government-owned information or such restricted information which stored in a system that is subject to protection under the law, a system owner (in the case of electoral IT systems, the CEC) should report to the SSAAS or its regional office all cases of unauthorised attempts to access such data.

Recently, in June 19, 2019 Cabinet of Ministers of Ukraine has approved a resolution about the general cybersecurity requirements for the critical infrastructure\textsuperscript{14}. These general cybersecurity requirements are universal for all critical sectors. Ministries and other central

\textsuperscript{12} CEC Resolution On the Procedure for the Use of the Information and Analytical System “Elections of the President of Ukraine” by the district electoral commissions for the election of the President of Ukraine of the Unified Information and Analytical System “Elections”, April 28, 2014 No. 392, available at: https://zakon.rada.gov.ua/laws/show/v0392359-14

\textsuperscript{13} The contract for 510,906 EUR was concluded on January 2019. Article 6 of the contract describes the required works and services. The copy of the agreement is available on the state procurement platform Prozorro.

\textsuperscript{14} https://translate.google.com/translate?depth=1&url=translate.google.com\textsc{com}&sl=uk&tl=en&u=https://zakon.rada.gov.ua/laws/show/578-2019-%D0%BC%s=%D0%BCs\textsc{F&fvid=17259,15700223,15700186,15700190,15700258,15700259,15700262,15700265#n8
executive bodies may develop specific requirements, taking into account the sectoral specifics of the functioning of critical infrastructure objects that relate to their area of responsibility, but such requirements have to be approved by the SSSCIP. Although the Law on the Basic Principles of Cybersecurity has been complemented recently, it is vital that the list of the state’s critical infrastructure objects will be agreed by the Cabinet of Ministers as soon as possible. Without the existence of the list of critical infrastructure objects, the responsibility for implementing general security requirements is still not formalised.

CYBERSECURITY STRATEGY (2016)

The national cybersecurity strategy was approved by the President of Ukraine in 2016 and it preceded the adoption of cybersecurity law. Between 2016-2018, this strategy was the sole national legal act in Ukraine addressing cybersecurity. It outlines threats to Ukrainian cyberspace and sets out strategic objectives and concrete actions to achieve resilience, reduce cybercrime, develop cyber defence policy and capabilities, develop industrial and technological resources, and to establish a coherent Ukrainian position with regards to international cyberspace policy. The strategy is supplemented by annual action plans that are issued by the Cabinet of Ministers.

The purpose of the 2016 cybersecurity strategy was to create conditions for the safe functioning of cyberspace and its use in the interests of the individual, society and the state. To achieve this goal, it was necessary to create a national cybersecurity system. The strategy thus set up a national cybersecurity governance framework, which was subsequently transposed into the cybersecurity law.

The strategy addresses challenges related to electoral IT systems and their effective protection during election periods. Two threats described in the strategy are particularly relevant to this report: an insufficient level of coordination, interaction and information exchange between actors providing cybersecurity in both the public and private sector; and the insufficient development of organisational and technical infrastructure, which can thereby hinder the cybersecurity of critical information infrastructure and governmental electronic information resources.

Above all, the strategy focuses on national security and military aspects of cybersecurity, which fall under the mandate of the National Security and Defence Council (NSDC). However, it does not address the protection of critical sectors of national economy, consumers and businesses from cyber attacks. Nor is it clear who is to monitor the implementation of the strategy. Potentially, this could be conducted either, which develops proposals for the President and acts as a coordinator of activities in the field of critical infrastructure protection, or it could be the Cabinet of Ministers, which implements national policy in the field of cybersecurity and provides resources for the functioning of national cybersecurity system.

LAW ON THE PROTECTION OF INFORMATION IN INFORMATION AND TELECOMMUNICATION SYSTEMS (1994, UPDATED IN 2014)

This law provides definitions of key information protection terms, outlines assets subject to protection, and describes the parties related to the process of information protection. The law defines the powers of government agencies, conditions for processing information, and relations between information owners and system owners. Eighteen relevant terms and concepts are defined by this law, including the information owner, the protection of information, information blocking, destruction, etc. Importantly, the concept of integrated information protection system is defined as a complex of administrative and engineering measures, techniques, and methods to protect information.

According to this law, the responsibility for ensuring information security of a system relies on the owner of that system. In the case of government-owned information or restricted information that is subject to protection under the law, a system owner must establish an information protection service or appoint persons responsible for managing and supervising information protection. For the electoral system, the owner is the CEC. This kind of dispersed responsibility prescribed by law, however, is detrimental to the cybersecurity of those systems and the security of the supersystem itself as it impedes knowledge sharing and leads to limited financing of cybersecurity initiatives.

RELATED LEGISLATION, DECREES AND PROCEDURES

There are several laws related to cybersecurity and the responsibilities of stakeholders, for example, the Law on the State Service of Special Communications and Information Protection, the Law on the Security Service of Ukraine, but also the Laws on the Fundamentals of National Security and the Law on Information.

In addition to those laws, the government and the SSSCIP have adopted a number of resolutions to increase resilience and enhance cybersecurity. These are related to the global data transmission networks used by government agencies, including the CEC. Such complementary rules are:

- Rules on the provision and receipt of telecommunication services
- Guidelines on how to connect to global data network
- Rules on providing information security in information and telecommunication systems
- Cooperation procedures between the executive authorities on the protection of state

In the context of electoral ICT systems, two resolutions play an especially important role. Firstly, the procedure for establishing the list of the state’s CII objects. It is of high importance because it defines the priority areas of cyberdefence. The procedure is a governmental legislative document which has not yet been passed and its first version is currently (as of August 2019) in preparation. The list of CII objects needs to be approved by the government and its formation is legally the responsibility of the SSSCIP. However, the process of developing the first drafts of the list has shown that in practice it is developed in cooperation with other stakeholders, notably the SSU.

The second noteworthy regulation is the procedure for assessing the security of state information resources. It specifies that the authorised central executive agency for special communications management and information protection (i.e., the SSSCIP) issues certificates that prove compliance to the complex of administrative and engineering measures, techniques, and methods to protect information. Both main electoral ICT systems – Vybory and SVR – have passed the assessment and have been certified by the SSSCIP. This certification is a prerequisite for the operation of a state information system.

### 3.4 Key Players in National Cybersecurity

The adoption of the Law on the basic principles of cybersecurity defined the key stakeholders and their roles, and set the responsibility for the co-ordination of cybersecurity activities related to national security to the President of Ukraine. The President implements this task via the national cybersecurity co-ordination centre, which is part of the permanent structure of the National Security and Defence Council, a high-level coordination body for national security (including cybersecurity). However, the lack of clarity regarding when presidential level mechanisms should be invoked prevents Ukrainian cybersecurity stakeholders from reaching a consensus on interagency cooperation at strategic, operational, and tactical levels.

Regarding, for example, who shall coordinate such cooperation and which organizations should be involved. In contrast, a good example is CERT-UA and SSU co-operation in investigations of cyber incidents, where CERT-UA is a lead national authority, but major (e.g., Advance Persistent Threat-level) cyber incident investigations are conducted by the SSU.

The key public agencies mandated to deal with cybersecurity are the National Security and Defence Council with its National Coordination Centre for Cybersecurity, the Parliament of Ukraine with its Standing Committee for Informatisation and Communications, the State Service for Special Communications and Information Protection (SSSCIP), the Security Service of Ukraine (SSU), the Department of Cyber Police within the National Police, the Ministry of Defence and the General Staff of the Armed Forces, intelligence agencies and the National Bank. Figures 1 and 2 depict the organization of the cybersecurity system in Ukraine. For more detailed competences of each institution, see Annex II.

![Figure 1. Key public stakeholders in the Ukrainian national cybersecurity system](image)

---

19 Resolution of the Cabinet of Ministers on Approval of the Procedure for the Cooperation of Executive Bodies, 2006 No. 373, [http://zakon4.rada.gov.ua/laws/show/373-2006-%D0%BF](http://zakon4.rada.gov.ua/laws/show/373-2006-%D0%BF)


National Coordination Centre for Cybersecurity (the NCCC) of the National Security and Defence Council coordinates and supervises the activities of the entities responsible for cybersecurity. Set up in 2016, the NCCC’s board is comprised of the heads of multiple organisations: the First Deputy or Deputy Minister of Defence, the Chief of the General Staff of the Armed Forces, the Head of the SSU, the Head of the Foreign Intelligence Service, the Head of the National Police, the Head of the National Bank as well as the Head of the Main Directorate of Intelligence of the Ministry of Defence, the Head of the Office of Intelligence of the Administration of the State Border Guard Service, and the Head of the SSSCIP. The NCCC works according to an action plan prepared every few months including practical tasks for all institutions represented. More generally, the National Security and Defence Council provides recommendations to the President.

Standing Committee for Information and Communications at the Parliament initiates legislation and reviews draft laws on cybersecurity that are submitted to the Parliament.

State Service for Special Communications and Information Protection.
The State Service for Special Communications and Information Protection (SSSCIP) is the technical security and intelligence service under the control of the President of Ukraine.

CERT-UA or the Ukrainian Government Response Team for Computer Emergencies is a unit structurally related to the State Centre for Cyber Defence. CERT-UA prevents and mitigates the effects of cyber attacks. For example, if hackers attack the CEC’s servers or the President’s website during an election, CERT-UA’s specialists will respond and help to mitigate and remediate the consequences. CERT-UA will contact international response centres, trace the source of the threat and cooperate with other Ukrainian computer emergency response teams (CERTs) in the financial sector or elsewhere, as well as with private cybersecurity enterprises. The CERT-UA team processes information received from citizens about cyber incidents during elections and assists local government bodies, military organisations, enterprises and institutions in countering cyber threats. Data on electoral cyber incidents is collected, analysed and stored in CERT-UA’s incident register.

State Centre for Cyber Defence was established in 2018 and it operates within the SSSCIP as a practical mechanism for early detection of cyberthreats and effective counteraction to cyberattacks. The Centre carries out information security audits of critical infrastructure objects and ensures the functioning of vulnerability detection and the cyber incident response system.

Security Service of Ukraine and its Centre for Cyber Security
The Security Service of Ukraine is tasked with the prevention, detection, countering and investigation of cyber threats that can inflict damage on the level of national security. It has a strong counterintelligence mandate in combating cyber terrorism and cyber espionage. The SSU operates one of the three Ukrainian public Security Operations Centres (SOCs), while the SSSCIP and the Armed Forces General Staff operate the other two SOCs that provide cyber threat detection and mitigation capabilities through the use of sensor infrastructure. The SSU is also authorized to conduct discreet and unannounced security checks to test the resilience of critical infrastructures against cyber attacks.

The SSSCIP issues certificates that prove compliance to the information protection systems – such as, compliance to the complex of administrative and engineering measures, techniques, and methods to protect information. For example, the SSSCIP has the task to check and, if compliant, to issue certificates to the most important electoral IT systems, such as Vybory.

CERT-UA and the State Centre for Cyber Defence are part of the SSSCIP and implement organizational and technical measures to prevent, detect and respond to cyber incidents and cyber attacks and mitigate the damage. They are also tasked with the provision of information on cyber threats and recommendations on security measures.

It takes care of the technical protection of state information resources and information in cyberspace. The SSSCIP maintains and operates the national telecommunication network, which provides secure communications to public authorities and is used as an emergency communications network. The SSSCIP also has a co-ordinating role at the operational level by setting requirements and overseeing information security audits at critical infrastructures. The SSSCIP also licenses companies that have the right to provide cryptographic protection and technical information protection services.

The protection of public institutions (like the CEC) and critical infrastructure are technically and organisationally covered first and foremost by the SSSCIP and the SSU. The private sector and commercial institutions are covered by the cyber department of the National Police. The National Bank plays an important role regarding the cyber defence system in the banking sector; but it has no direct influence over electoral cybersecurity and thus is excluded from the current analysis. The Ministry of Defence, Armed Forces and intelligence agencies do not have mandates for securing electoral cybersecurity except in cases of military aggression in cyberspace.

The SSSCIP issues certificates that prove compliance to the information protection systems – such as, compliance to the complex of administrative and engineering measures, techniques, and methods to protect information. For example, the SSSCIP has the task to check and, if compliant, to issue certificates to the most important electoral IT systems, such as Vybory.

CERT-UA or the Ukrainian Government Response Team for Computer Emergencies is a unit structurally related to the State Centre for Cyber Defence. CERT-UA prevents and mitigates the effects of cyber attacks. For example, if hackers attack the CEC’s servers or the President’s website during an election, CERT-UA’s specialists will respond and help to mitigate and remediate the consequences. CERT-UA will contact international response centres, trace the source of the threat and cooperate with other Ukrainian computer emergency response teams (CERTs) in the financial sector or elsewhere, as well as with private cybersecurity enterprises. The CERT-UA team processes information received from citizens about cyber incidents during elections and assists local government bodies, military organisations, enterprises and institutions in countering cyber threats. Data on electoral cyber incidents is collected, analysed and stored in CERT-UA’s incident register.

State Centre for Cyber Defence was established in 2018 and it operates within the SSSCIP as a practical mechanism for early detection of cyberthreats and effective counteraction to cyberattacks. The Centre carries out information security audits of critical infrastructure objects and ensures the functioning of vulnerability detection and the cyber incident response system.

Security Service of Ukraine and its Centre for Cyber Security
The Security Service of Ukraine is tasked with the prevention, detection, countering and investigation of cyber threats that can inflict damage on the level of national security. It has a strong counterintelligence mandate in combating cyber terrorism and cyber espionage. The SSU operates one of the three Ukrainian public Security Operations Centres (SOCs), while the SSSCIP and the Armed Forces General Staff operate the other two SOCs that provide cyber threat detection and mitigation capabilities through the use of sensor infrastructure. The SSU is also authorized to conduct discreet and unannounced security checks to test the resilience of critical infrastructures against cyber attacks.

In addition, the SSU has investigatory powers of cyber incidents and cyberattacks against government information systems and CIIs during election periods.
The Centre for Cyber Security was established in January 2018 as the unit structurally related to the SSU's department of counterintelligence and protection in the sphere of information security. The Centre has a mandate to prevent cyber attacks against critical infrastructure and public services. The Centre has its own computer forensics and cyber incident laboratory. The Centre’s equipment and software were acquired with the help of the Ukraine-NATO fund.

Cyber Police Department
The Cyber Police Department of the National Police has been operational since 2015. It is tasked with the prevention, detection, countering and investigation of cyber crimes as defined by the Penal Code and that do not fall within the national security domain (such as, for example, e-payment fraud, crimes on the Internet, child abuse, and infringement of copyright). Additionally, the department is responsible for raising cyber awareness among the public. A local cybercrime unit exists in every region of Ukraine.

The various cybersecurity agencies and units of the governmental may invite experts from the Forensic Science Centre of the Ministry of Interior when it is necessary to collect and analyse digital evidence. The experts can take part in collection, seizure, storage, analysis, examination and evaluation of digital evidence.

4. ASSESSMENT OF THE IT INFRASTRUCTURE

By threats we mean anything that can exploit a vulnerability of an IT system, intentionally or accidentally. Risk refers to the potential for loss or damage when a threat exploits a vulnerability. Threats may exist, but if there are no vulnerabilities then there is little risk.

4.1 THREATS TO THE STATE VOTER REGISTER

The State Voter Register, continuously monitored by the CEC, is an important system for carrying out elections. The critical period for the SVR is some weeks before elections when voters are actively checking their records and several amendments are made in the SVR by RMBs.

Based on the information obtained during meetings with the SSU, the CEC and other related stakeholders, the main threats to the SVR include:
1. compromise of the information accumulated and processed in the systems in order to obstruct the implementation of electoral procedures (for example, delay in the formation of voter lists in the regions); and
2. unauthorised change or modification of the information of the SVR with the aim of compromising voters’ lists and creating grounds for appeal of election results.

In December 2018 ODIHR/OSCE interlocutors emphasised the importance of preventing and responding to possible foreign interference in the upcoming election campaign and noted concerns with potential cyber threats to election infrastructure, potential negative effects of disinformation during the campaign period, as well as potential misuse of administrative resources during the campaign. ODIHR/OSCE raised concerns about the accuracy and timely updates of the voter lists, specifically referring to the data on internally displaced persons, internal labour migrants and citizens living abroad.

Based on our observations, interviews with stakeholders and research, no major incidents interrupted the electoral procedures during 2019 presidential elections. However, the SVR’s online service Voter’s Cabinet experienced load problems before the elections due to a high number of online users checking their data in the register. SVR users have access to the system through an internal network and not the public Internet. Therefore, DDoS is not a risk for keeping the SVR up to date. However, voters are able to check their status and their polling stations in the SVR through the Internet. This offers a perimeter that is wider and more open to various attacks and overload. Before and during the 2019 elections, voters were actively checking their records online using the service Voter’s Cabinet and requested amendments to their records at the RMB of their current residence. According to the CEC, Voter’s Cabinet experienced a large load before elections. Furthermore, the number of voters’ appeals to the SVR was very high.

The centralised telecommunications architecture of the SVR puts a heavy load on central servers and telecommunications infrastructures that are used to connect these servers. Besides cyber threats, physical damage such as cutting electoral or network cables off from the central data centre is a serious potential threat (see Figure 3).
4.2 PROTECTION MEASURES FOR THE STATE VOTER REGISTER

The CEC has been continuously implementing measures aimed to enhance the security and the functionality of the SVR. In order to ensure the reliable operation of the SVR, additional security measures were implemented prior to elections to update and introduce new methods and technologies, modern software and hardware security of information, as well as to update the system infrastructure as a whole.

For data transmission, the network of JSC "Ukrtelekom" is used. The data transmission is protected by cryptomodules. All SVR workstations are connected to the common domain drv.gov.ua and two-factor authentication is used by administrators centrally but also at RMBS and RABs. The system construction involves three layers: a thin client (Internet browser), application server (web-server) and central database server. The administration of the SVR at the CEC contains a specialised department for information security.

In 2017 the SSSCIP conducted a security assessment of the SVR based on the national methodology and standard for IT security. Results of the examination testified that the provided system protection of information is in compliance with the requirements of Ukrainian normative documents. The compliance certificate No. 15638 was issued by the SSSCIP on 25 September 2017 and is valid until 2020. The SSSCIP also conducted two vulnerability checks of the system.

4.3 THREATS TO VYBORY

The CEC is single-handedly responsible for managing the security of the networks used for electoral IT systems. Since the CEC’s main task is to organise elections, it has limited resources to guarantee network security, which increases the risks to Vybory. The protection of network infrastructure is complicated, and thus up-to-date expert knowledge and help is needed from institutions responsible for cybersecurity on a national level.

4.4 PROTECTION MEASURES FOR VYBORY

To guarantee electoral cybersecurity, the CEC has taken the following steps:
• Installation of a modern network and information security equipment;
• Modernisation of the entire information security system; and
• Examination of the comprehensive information security system.

In January 2019, the CEC purchased services from the Ukrainian Scientific Development Enterprise Medirent Ltd for updating Vybory software. Updates were needed to bring the system into accordance with the requirements of the current legislation and to optimise its work based on experiences from the actual operation of the system.

In 2019, the SSSCIP performed a security assessment of Vybory (including on the regional level) and the CEC web servers. The aim of the testing was to identify vulnerabilities that might allow cyber attacks and incidents. The assessment included penetration testing of the CEC’s internal network (as Vybory is located there) and an assessment of the architecture of the system. The inspection of the Vybory system by working groups was carried out according to the methodology developed by the owner of the Vybory. Similarly to the security assessment of the SVR, the assessment of Vybory was based on the national methodology and standard for IT security. The assessment was conducted by private companies, although the SSU was also involved.

The timeframe of the assessment was potentially too narrow, as the latest version of Vybory was completed less than two weeks before elections. Once the assessment was performed, the SSSCIP issued recommendations to the CEC for improving the system’s security. After the assessment on 22 March 2019 the SSSCIP issued Vybory a security certificate, confirming the system’s compliance with technical requirements for information security.
Laws and resolutions provide measures in case of the dysfunction of the Vybory system. In case of any problems in the process of transmitting information to the CEC, the Vybory administrator is obliged to immediately alert the technical support service. On election day, voting information may be transmitted by telephone or fax if the Vybory system is not available. After the restoration of the system, the system administrator is obliged to enter all the data transmitted by alternative means back into Vybory. These are reasonable measures that guarantee information flow, even if some incidents do occur.

4.5 TRAININGS AND EXERCISES

In February 2019, the CEC organised a two-day training exercise of the Vybory system for all 199 DECs. The event was arranged together with the system’s developer, Scientific Development Enterprise Medirent Ltd. This exercise aimed to familiarise DECs with the deployment and operation of the system, the monitoring of its status, and solving problems that may arise while operating it. Further, technical and organisational issues within information security were discussed. At the end of the programme, the main rules of technical support and interaction procedures between system administrators and technical support were approved.

Additionally, representatives of the CEC Secretariat and the SVR (about 20 employees) have been trained on leading cyber hygiene practices. Similar training was offered to a wide range of electoral stakeholders, including representatives of civil society and DEC members and staff prior to elections. Several cyber hygiene training sessions were held with representatives of NGOs and the media, and with electoral process managers. The events were organised by the CEC with the support of the IFES, USAID and UK Aid. Participants learned about guidelines for online security and acquired skills through which to counteract phishing attacks. In addition, participants studied cyber hygiene best practices in the public sector during the presidential election, and also considered relevant information protection issues. All participants received the appropriate certificates, following the completion of a final test.

In March 2019, cybersecurity training was conducted which simulated real situations and taught measures to prevent, detect and respond to cyber incidents and cyber attacks in relation to information systems of the CEC, as well as to eliminate their negative consequences. Two protection teams were formed: the first consisted of employees of the SSU and the CEC, the second of the SSSCP.

No major incidents interrupted the electoral procedures during 2019 presidential elections. However, human risks (insider threats) are high; new people will be recruited and efficient training is needed before every election. Training and awareness-raising activities are needed for thousands of employees that are working with SVR and Vybory.

4.6 RISKS AND RECOMMENDATIONS

The CEC, including the SVR and the DEC employees around the country are constantly being targeted as an entry point into organisations’ systems and networks. The real way to avoid staff-related breaches is via thorough education, awareness-raising and the effective enforcement of policies and procedures.

A detailed overview of risks and recommendations regarding IT infrastructure for organising elections is described in the table below.

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk Description</th>
<th>Recommendation</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outdated IT infrastructure security measures do not correspond to relevant latest threats and risk assessments as the landscape of cyber threats is rapidly changing and new vulnerabilities are constantly discovered.</td>
<td>To regularly conduct risk analysis and vulnerability assessment of electoral IT systems. Analysis of previous incidents should be considered a valuable source of information for updating risk analysis.</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To regularly review threat models that also include risk descriptions and scenarios of the CEC’s internal network; to regularly conduct pen-tests. Certificates must be renewed because the environment and requirements change in every election.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk analysis should be followed by implementing timely mitigating measures to protect IT systems from cyber threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outdated physical security measures do not correspond to relevant latest threats and risk assessment. Considering that a large number of DECs (199) around the country are using Vybory and around 680 RMBs work on the SVR, physical risks are unquestionable.</td>
<td>To assess the physical risks to infrastructure (including workstations). Besides cyber threats, physical damage such as cutting electoral or network cables off from the central data centre is a serious potential threat due to centralised architecture.</td>
<td>High</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>Assigning too low of a priority to the protection of electoral systems that may result in insufficient resources to identify, analyse and recover from cyber incidents.</td>
<td>To include the CEC (and Vybory and SVR) in the official list of the state's critical infrastructure which is currently in preparation by the SSSCIP and due to be passed by the government. This would prioritise the protection of the CEC's IT systems and provide additional resources for the CEC.</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Inability to hire and retain competent IT security personnel.</td>
<td>To ensure additional finances to the improvement of the CEC's networks and IT systems like SVR and Vybory. This can be done through the State Budget of Ukraine, but also through technical assistance from international organisations and funds. Cyber hygiene trainings and awareness-raising activities are needed for employees who are working with SVR and Vybory. Competitive salaries and attractive working conditions for cybersecurity personnel are required to hire educated and experienced staff.</td>
<td>Medium</td>
</tr>
<tr>
<td>5</td>
<td>Last minute changes to electoral ICT systems may compromise their integrity, confidentiality and availability.</td>
<td>To insert into electoral/SRV laws a clause prohibiting rapid changes to electoral laws and procedures that have direct influence on the functionality and security of electoral IT systems. The law should state that 6 months before the election day, no major changes in electoral administration, nor its ICT systems are allowed.</td>
<td>Medium</td>
</tr>
<tr>
<td>6</td>
<td>Ineffective security measures applied to the CEC network</td>
<td>To allow public institutions like the CEC to use a secure environment (i.e. a special virtual network) that is centrally managed and monitored by competent authorities. One possible solution could be the use of the National Telecommunications Network, maintained by the SSSCIP, that provides secure communications to public authorities and is used as emergency communications network. The CEC currently manages networks on its own.</td>
<td>Medium</td>
</tr>
<tr>
<td>7</td>
<td>Ineffective identification of human error and cyber attacks, including insider threats</td>
<td>To implement a system of logging, monitoring and log analysis for Vybory and the SVR to discover and manage possible human error and insider attacks.</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>Low availability of electoral IT systems</td>
<td>To develop contingency plans for data centres used to host or support electoral IT systems. Countermeasures and alternatives should exist for cases where hosting suffers major service interruption or power supply problems.</td>
<td>Low</td>
</tr>
</tbody>
</table>

### 5. ASSESSMENT OF INTERAGENCY COOPERATION

In the EU, interagency cybersecurity crisis management is traditionally divided into technical, operational and strategic/political levels. The current report focuses on the technical and operational levels. For effective solutions, coordinated response, shared situational awareness and public communications are important. At the outset, based on the information obtained during various stakeholder interviews, the most critical missing component seemed to be the technical capability of the CEC. The CEC is a small organization with only a few technicians covering elections-related systems across the country.

#### 5.1 COOPERATION BEFORE AND DURING THE 2019 ELECTION

After the cyber incidents during the 2014 election, all stakeholders responsible for cybersecurity in Ukraine, including the CEC, recognized that ensuring the cybersecurity of the 2019 presidential election would be a crucial issue. Already in early 2018, CEC chairperson...
In setting up the operational task force, the following preparatory measures were taken:

a. In order to implement the most efficient protective measures against cyber attacks, the SSSCIP conducted threat modelling of the elections that also included risk descriptions and scenarios.

b. the SSU, in cooperation with the CEC, developed technical measures for protecting the CEC’s infrastructure against cyber incidents and attacks, and for raising the cyber defence level of the CEC systems. The SSU, covering critical infrastructures of the country, was a key player in ensuring efficient incident handling during a cybersecurity crisis and having incident monitoring and surveillance capacity, including continuous analysis of threats and risks on a technical level. Cooperation projects were implemented in the framework of both EU assistance, as well as the NATO-Ukraine Trust Fund on Cyber Defence.

c. The CEC upgraded its information technology infrastructure: it renewed firewall and antivirus, added new SIEM logging and monitoring system, and introduced additional tools for CEC services users to avoid opening or executing files containing malicious elements. The procurement and implementation of certain technical equipment was carried out with the support of the USAID Mission in Ukraine with the involvement of the International Foundation for Election Systems (IFES).

In addition, the CEC ordered all 199 DECs to form interagency working groups to verify Vybor’s security, including its elements installed in the premises of the DECs. The working groups also included employees of the SSSCIP and the SSU. The reports of the working groups were delivered to the CEC, as well as to the SSSCIP. The SSSCIP inspected the devices on regional level and compiled relevant reports. According to the CEC, main actor in the working groups was the SSSCIP as they checked the networks and gave assurances that systems are in accordance with the requirements. The role of the SSU was more flexible.

Since the CEC and the SSSCIP worked together in the operational centre during election period, the SSSCIP had direct access to the information and the incidents. This kind of cooperation and direct channel for information sharing ensured rapid response in case of a major incident. Thanks to election observation and smooth information flow from the CEC towards the public, no major incidents occurred during elections that would have stymied voting or counting procedures.

All in all, the measures taken for coordinated incident response and network monitoring during the election period were appropriate.

**5.2 RISKS AND RECOMMENDATIONS**

The key players in interagency cooperation for elections are the CEC, the SSSCIP and the SSU. These three organizations are key incident responders at technical and organizational levels in the case of cybersecurity incidents and they establish close cooperation as soon as incidents happen. Building on the successful mitigation of risks and challenges during the presidential election of 2019, the table below provides recommendations for the improvement of the cybersecurity of elections via the improvement of interagency cooperation practices.
6. CONCLUSIONS

Today’s Ukraine’s security situation has fundamentally shifted compared to pre-2014 era. This has taken place not only in the traditional spheres of national security, but also in a great extent with regards to cybersecurity. The 2014 presidential election of Ukraine, which saw an unprecedented number of successful attacks on the electoral IT systems, sent an obvious alarm that there is a need for broadranging improvements of the organisational and technical sides of cybersecurity. Without such improvements, the integrity of democratic institutions would permanently undermined.

Following 2014, the Ukrainian parliament and the government with its various agencies initiated substantial action plans to tackle the weaknesses of election cybersecurity – notably, the first cybersecurity strategy and the first comprehensive cybersecurity law were passed. But also a plethora of technical and updates were made to the IT systems of the Central Election Committee, the institution responsible for the organisation of elections. Some significant milestones (for example, a CEC resolution on organisational aspects of Vybory, a key IT infrastructure) were, in fact, reached even only a few weeks before the 2019 presidential election.

Taking into account the recent improvements in cybersecurity, the current report has aimed to provide a fresh assessment of the cybersecurity situation of Ukrainian elections. The evidence suggests that, in general, the amendments to the cybersecurity system have significantly improved the operation and reliability of the system compared to that of in 2014. Notable improvements were seen in both of the objects of the current analysis (those being cybersecurity infrastructure and interagency cooperation). As a result, no major incidents had any permanent negative impact during the 2019 presidential elections, despite around 9000 potential threat cases (including a relatively sophisticated malware by the hacker group Dragonfly).

However, various gaps in cybersecurity were also identified. Most importantly, it must be highlighted that as cyber threats (including the technical specification of the threats) evolve on a daily basis, the defence systems must be regularly reviewed and updated. The existing
The mechanisms of election cybersecurity in Ukraine do not yet specifically address this issue. The report altogether identified 12 different risks – to which corresponding mitigation recommendations were given. This list also included the recommendation on adding the CEC (and its constituent IT systems: Vybor and the State Voter Register) within the list of the state’s critical information infrastructure which is currently in preparation and due to be passed by the government. The report considers this inclusion as a fundamental requirement for ensuring permanent and sufficient attention on election cybersecurity in Ukraine.

ANNEX I - EXTERNAL RESOURCES ON ELECTORAL CYBERSECURITY

Since 2016, there has globally been a growing focus on election cybersecurity. This has led to a number of instructive materials and best practices. This section lists some resources that might be particularly useful for Ukraine. The list is a starting point, not a comprehensive one.

Cooperation

A key aspect of election security is interagency cooperation. Given the evolving nature of the field, the most helpful examples come from emerging practices across the world. In particular, it might be instructive to look at:

- The election security work done under the auspices of the Swedish Civil Contingencies Agency (MSB), the national civil defence agency under the Ministry of Defence. This includes interagency cooperation and vulnerability assessment, as well as training to prepare against various threats to elections, taking a whole-of-society approach;
- The Elections Infrastructure Information Sharing and Analysis Centre (EI-ISAC), operated by the Centre for Internet Security in the US, is a central point for sharing information, analysis, and situational awareness for cyber threat prevention, protection, response, and recovery;
- The European Union established a Rapid Alert System to tackle disinformation by facilitating information exchange and response coordination.

Playbooks, checklists and instructional resources

The following may also prove useful:

- The European Union’s Network and Information Security Directive’s Compendium on Cybersecurity of Election Technology;
- Belfer Center, Defending Digital Democracy Project, The State and Local Election...
Cybersecurity Playbook with accompanying thematic playbooks:
• The Global Cyber Alliance, Cybersecurity Toolkit for Elections.

ANNEX II - COMPETENCIES OF THE MAIN NATIONAL CYBERSECURITY STAKEHOLDERS

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Acronym</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>President</td>
<td>NSDC</td>
<td>Coordination of cybersecurity nexus activities as a component of national security</td>
</tr>
<tr>
<td>National Security and Defence Council</td>
<td>NCCC</td>
<td>Coordination and oversight of the security and defence sectors operating in cybersecurity</td>
</tr>
<tr>
<td>Security Service of Ukraine (including its Centre for Cyber Security)</td>
<td>SSU</td>
<td></td>
</tr>
</tbody>
</table>
- Prevention, detection, remediation and exposing of crimes against peace and security of humankind committed in cyberspace;  
- Counter-intelligence and operational search activities aimed at combating cyber-terrorism and cyber-espionage, secretly checks the readiness of critical infrastructure objects for possible cyber attacks and cyber incidents;  
- Countering cybercrime;  
- Investigation of cyber incidents and cyber attacks on state electronic information resources, information protection requirements established by law, critical information infrastructure;  
- Responding to cyber incidents in the field of national security. |

30 https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook  
31 https://www.cisecurity.org/elections-resources/  
32 https://gcatoolkit.org/elections/  
33 According to the Law on the Basic Principles of Cybersecurity
| State Service for Special Communications and Information Protection of Ukraine (including its State Centre for Cyber Defence and CERT-UA) | SSSCIP | • Formation and implementation of national policy and requirements on the protection of state information resources and information in the cyberspace;  
• Defence of objects of critical information infrastructure, state control in these areas;  
• Coordination of activities of other entities providing cybersecurity regarding cyber defence;  
• Ensuring the creation and operation of the National Telecommunication Network, implementation of the organisational and technical model of cyber defence;  
• Organisational and technical measures to prevent, detect and respond to cyber incidents and cyber attacks and to eliminate their consequences;  
• Informing about cyber threats and appropriate methods of protection against them;  
• Implementation of the information security audit, establishment of the requirements for auditors, determination of the procedure for their certification (re-certification);  
• Coordination, organisation and conduct of security audits of the communication and technological systems of objects of critical infrastructure for vulnerability. |
| --- | --- | --- |
| National Police | • Ensuring the protection of human and civil rights and freedoms, the interests of society and the state from criminal encroachments in cyberspace;  
• Prevention, detection, remediation and disclosure of cybercrime, raising of public awareness of security in cyberspace. |
| Ministry of Defence and the General Staff of the Armed Forces of Ukraine | MoD | • Prepare the state against military aggression in cyberspace (cyber defence);  
• Military cooperation with NATO and other defence actors to ensure the security of cyberspace and to jointly protect against cyber threats;  
• Ensure cyber defence of critical information infrastructure in conditions of emergency and martial law. |
| Intelligence agencies of Ukraine | Intelligence activities concerning threats to the national security of Ukraine in cyberspace, other events and circumstances related to the sphere of cybersecurity. |
| National Bank | • Determination of the procedure, requirements and measures for the provision of cyber defence and information security in the banking system of Ukraine and for the entities of the transfer of funds, while exercising control over their execution;  
• Creation of a centre for cyber defence of the National Bank of Ukraine, provision of a cyber defence system for the Ukrainian banking system;  
• Evaluation of the state of cyber defence and information security audit on critical infrastructure objects in the banking system of Ukraine. |