Cybersecurity in Ukrainian Elections

June 2018

Assessment team:
Beata Martin-Rozumiłowicz, Carsten Schürmann, Yulia Shypilova, Victor Zhora, Goran Petrov

This report was prepared by the IFES’ Cybersecurity Assessment Team of the International Foundation for Electoral Systems (IFES) through the support of the United States Agency for International Development (USAID) and UK aid. The opinions expressed herein are those of the author and do not necessarily reflect the views of USAID, the United States Government, or the UK government.
# Table of Contents

Executive Summary ................................................................................................................................... 6  
Introduction .............................................................................................................................................. 8  
Background and Context ........................................................................................................................... 9  
The Legal Framework ................................................................................................................................ 11  
Cybersecurity Infrastructure in Ukraine .................................................................................................... 13  
Cybersecurity and the Election Administration ....................................................................................... 14  
The Results Management System (RMS) .................................................................................................. 16  
Cybersecurity and Election Audits ............................................................................................................ 18  
Recommendations .................................................................................................................................... 20  
Short-Term Recommendations .................................................................................................................. 20  
Long-Term Recommendations .................................................................................................................. 20  
Annex I: Meetings on cybersecurity with key stakeholders ................................................................. 22  
Annex II: Program of the Expert Round Table “Cyber Threats for the Electoral Process in Ukraine” ...... 23  
Annex III: List of participants of the Expert Round Table ...................................................................... 24
Executive Summary

Much has transpired regarding the cybersecurity situation in Ukraine since 2014. The conflict resulting from the occupation of Ukrainian territories has clear characteristics of hybrid warfare (including information warfare in the form of a disinformation campaign) and critical systems hacked into and destroyed through cyberattacks.

An important example includes the CEC cyberattack during the presidential election in 2014. Three days before the elections, cyber attackers disabled the CEC network nodes and wiped clean (deleted information from) numerous components of the election system, including the Results Management System, using advanced cyberespionage malware. The system was made operational again only due to the existence of an offline backup. Several improvements have since been introduced in the CEC IT systems; for example, the office components have been separated from the critical networks and the remote access is limited or blocked.

Legal instruments relating to cybersecurity on the international level are limited. A new Law on Cybersecurity came into force on 9 May 2018. The law defines overarching cybersecurity concepts, organizational and collaborative aspects, as well as explanation of authority and responsibility. The government has a deadline of three months to issue normative acts that are to include details of cybersecurity, for example the conduct of audits, but it is yet unclear what concrete steps have been taken in this regard.

The new law includes a concept of Critical Infrastructure (CI) for facilities/institutions that provide certain critical services to the state or citizens. Considering that the CEC is an independent institution, it may need to formally request to be designated as CI. Some interlocutors understand that the CEC will sign a Memorandum of Understanding with the State Service for Special Communications and Information Protection (SSSCP). The two main cybersecurity agencies (SSSCP and the Security Service of Ukraine, SSU) operate security centers, which allow for a redundant approach to detect cyber threats. They also cooperate with the CEC.

At present, Ukraine uses an information security framework adapted from the Canadian framework. It is likely, however, that imminent normative acts will provide for the obligation to use the ISO/IEC 27000 family of information security standards. It is unclear which, if any, operational cybersecurity framework will be stipulated and utilized. Information about any standardized framework that may be used should be included in the bylaws.

At present, the CEC does not have a formalized set of instruments for conducting a comprehensive security analysis in relation to system design and implementation, detailing all security assumptions. Most interlocutors stressed the need for election system penetration tests (pen
tests). An important concern is whether the CEC pen tests will be conducted with due diligence and in sufficient time before elections to address the potentially identified shortcomings. It is also a concern that pen tests may not be enough to assess the security of a system, as more advanced security goals and/or insider attacks are typically not considered during pen tests. From previous experience, the CEC tends to readjust the system architecture before each election, due to operational needs. A thorough test should be conducted after this point, although CEC’s plans were not clear in this regard.

Recently, the CEC launched a program for replacing outdated equipment. This process is very important, since certain outdated components can pose security risks. The CEC could alternatively assume a business strategy of using external hosting solutions, however, they informed the team that they intend to keep all system components and data in-house. Both NATO and the OSCE Project Coordinator’s Unit (PCU) have offered assistance in purchasing significant parts of the equipment. The purchase lists have been determined, though the procurement procedures have not started, except those procured by the OSCE. According to the SSU, the system components should be purchased by the end of August, to allow for sufficient time for all other preparation. Per NATO’s Liaison Office in Kyiv, this timeframe is not sufficient to overcome administrative procurement obstacles.

The CEC is experiencing mistrust from stakeholders. The mandates of most CEC members have long expired and new CEC members should be appointed as soon as possible. However, it is unlikely that there will be a new CEC by the end of summer. The expectation of CEC composition change reduces the effectiveness of its mandate, including in reaching decisions on future projects.

Some interlocutors stated that the CEC’s biggest problem is human capacity. Compensation for IT specialists is said to be insufficient, compared to the private sector, and leads to attrition of high quality workers. Several interlocutors also stated the importance of CEC staff training. Both advanced trainings and trainings for beginners could be considered. A training curriculum could be developed and proposed to the CEC. The recommendations in this report provide more detail regarding potential technical assistance on election cybersecurity.
Introduction

This report is an overview of cybersecurity issues surrounding electoral and other critical systems in Ukraine important for the conduct of elections. The intended audience of the report is those interested in cybersecurity issues in elections in Ukraine, more generally, and those following electoral developments in the region.

The team was led by Beata Martin-Rozumilowicz (Director for Europe and Eurasia at IFES, Washington D.C) and included Carsten Schürmann (Associate Professor at the IT University of Copenhagen), Yuliya Shypilova (Senior Electoral Advisor, IFES Ukraine), Victor Zhora, (CEO Infosafe IT, Ukraine) and Goran Petrov (IFES Cybersecurity Consultant).

The assessment consisted of meetings held with relevant stakeholders, a list of which is annexed to this report. Interviews took place from May 14-18 and June 4-8. Stakeholders included relevant state authorities, local NGO cybersecurity experts (affiliated with the Ukrainian Information Security Group), and companies involved in this field. The assessment team met with various representatives of the CEC on four occasions. In addition to discussing current issues, the team also learned of updates to the design of a new Results Management System, which may be implemented prior to upcoming presidential elections in March 2019.

On June 7, IFES organized a roundtable on cybersecurity in elections, with the participation of expert speakers. Following this roundtable, IFES has initiated the creation of an informal cybersecurity group in Ukraine to exchange ideas and be an information clearinghouse for practitioners. The list of participants and the agenda are attached to this report.
Background and Context

Much has transpired regarding the cybersecurity situation in Ukraine since 2014. The conflict resulting from the occupation of Ukrainian territories has clear characteristics of hybrid warfare (including information warfare in the form of a disinformation campaign) and critical systems hacked into and destroyed through cyberattacks. There has been a series of high-profile attacks on Ukrainian institutions, including the attack on the CEC IT systems in May 2014. This attack was followed by a number of other significant and well-known cyberattacks. Arguably, the two most significant attacks were the BlackEnergy and (Not)Petya malware attacks.

On December 23, 2015, three companies running the Ukrainian power grid were successfully attacked, leading to a temporary disruption in the supply of electricity. A total of 30 substations that supplied electricity to some 230,000 people were switched off for 1-6 hours. This was a complex cyberattack that started with the successful infiltration of BlackEnergy malware, through phishing of specific individuals (spear phishing).

On June 27, 2017, a malware called (Not)Petya infiltrated the networks of many Ukrainian institutions, including banks, government agencies and electricity firms; it also spread worldwide. It appears that (Not)Petya propagated through being planted as an update of a popular accounting software, MeDoc.¹

Specifically, with regards to elections, the most notorious attack came during the 2014 presidential contest. According to available information, three days before election day during the night from May 21-22, 2014, cyber attackers were able to access the CEC servers that they had previously compromised, disabled the CEC network nodes and wiped clean (deleted information from) numerous components of the election system, including the Results Management System (which was still in the testing mode). They were able to achieve this through the use of advanced cyberespionage malware.² They also deleted backups that were accessible online. This has been characterized as a high-level attack by cybersecurity experts, including by experts from CERT-UA.³

A Ukrainian-based group claimed responsibility for the 2014 attack on the CEC IT system, CyberBerkut.⁴

² The cyber experts from CERT-UA located the responsibility for creation of the malware to APT28. Available at: https://attack.mitre.org/wiki/Group/G0007
³ For more information, see the essay written by the CERT-UA representative at the time of the attack to APT28. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Koval_06.pdf. There are numerous other online resources, of which this article by the WSJ may be the most accurate description of events. Available at: https://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671
⁴ See the groups official website: https://cyber-berkut.org/en. More information about the group is available online, for example in the article: https://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902
They claimed at the time that they had exploited a vulnerability in the hardware of the router used by the CEC,⁵ which was not previously disclosed (a so-called zero-day vulnerability). The CERT-UA expert who reviewed the logs of the router told the assessment team that the logs show communication with external IP addresses belonging to hackers. At the time, Cisco reviewed the documentation and announced they have not found any vulnerability. However, recently, vulnerability in Cisco ASA series equipment has been discovered.⁶ According to the information available to the pre-assessment team, this dated but crucial piece of hardware, which is no longer supported by Cisco, is still located in the CEC, but is probably being replaced. The CEC, including through the help of its IT subcontractors and CERT-UA, managed to rebuild the Results Management System just one hour before the polls were opened on election day. This was achieved from back-ups that had not been exposed to the attacks.

The attack was followed with a significant DDoS attack on the system, which the CEC fended off. In addition, the results website on the internet-facing results server was also defaced, which showed the winner of elections being a right-wing politician.⁷ However, the compromised webpage was not linked from anywhere and was not in use, so it was immediately made clear that it was a website defacement and disinformation campaign, which had not been properly executed.⁸

According to one interlocutor working with the CEC, a lot of improvements have been introduced in the CEC IT systems in recent years, both conceptual and related to individual components of the system. For example, the office components have been separated from critical networks and remote access is limited or prohibited, depending on the system. A network flow monitoring solution has been implemented, as well as modern intrusion prevention systems. A new disaster recovery data center has been established and endpoint authentication mechanisms have been implemented over the CEC local network. At present, there is a significant level of support both in terms of cybersecurity and elections from various inter-governmental and development aid agencies.

In January 2018, MITRE a not-for-profit organization that conducts research on behalf of the U.S. government, made an assessment and proposed a set of recommendations on Ukraine’s cybersecurity strategy. Their overall assessment is that the country “has established realistic strategic objectives in cyber, and possesses the technical talent to achieve them if these

---

⁵ Cisco Adaptive Security Appliance - ASA.
⁶ See this report from Cisco. Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
⁷ See the article for more information: https://www.kyivpost.com/article/content/war-against-ukraine/inforesist-security-service-of-ukraine-says-russia-is-behind-hacking-of-the-website-of-the-cec-and-cec-system-elections-349715.html
⁸ It appears that the false webpage was shown on Russia’s First TV Channel 15 minutes after it was accessed and checked it was still there where it was planted, which was proved by web server logs.
advantages are leveraged by a commitment to change through focused, disciplined and collaborative efforts.\textsuperscript{9} MITRE identified three areas of risk: operational resilience, uncompetitive wages for the cybersecurity workforce, and intra-governmental cooperation.

The Legal Framework

Legal instruments referencing cybersecurity on the international level are limited. Ukraine has ratified the Convention on Cybercrime of the Council of Europe (the Budapest Convention) in 2006. The Budapest Convention is the first international instrument with an objective to establish a common criminal policy to protect against cybercrime by adopting relevant domestic legislation and fostering international collaboration.\textsuperscript{10}

Article 17 of the Ukrainian Constitution, amongst others, states that information security is one of the most important functions of the state and a matter of concern for all Ukrainians.\textsuperscript{11} Information security is largely bundled with cybersecurity concerns, although the new legislation more clearly distinguishes between the two.

There is no direct crossover between elections and cybersecurity or information security in any law. Apart from the Constitution, the legal election framework includes pieces of legislation, including individual laws for different types and components of elections: presidential, parliamentary and local, the Law on the CEC and the Law on the State Voter Register. Also of importance are The Code of Ukraine on Administrative Offences and the Criminal Code.\textsuperscript{12}

The new Law on the Fundamental Principles of Providing Cybersecurity of Ukraine (hereinafter: Law on Cybersecurity) was signed by the President on 5 October 2017 and came into force six months after promulgation, on 9 May 2018.\textsuperscript{13} The law defines overarching cybersecurity concepts, organizational and collaborative aspects, as well as explanation of authority and responsibility. It also explicitly notes that cybercrime is punishable by law.

\textsuperscript{10} The Budapest convention is in force in Ukraine since 1 July 2006. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
\textsuperscript{11} The translation of the Constitution is available at: https://www.nist.gov/file/270221
\textsuperscript{12} The chapter XI of the Criminal Code contains provisions for prosecution of attacks on computer systems and networks. Available at: http://www.legislationline.org/documents/action/popup/id/16257/preview
\textsuperscript{13} The text of the law is available at: http://www.profiaudit.com.ua/images/newzak/17/131117G.htm
Furthermore, the law provides for the concept of critical infrastructure (CI), which may include institutions and facilities that provide services in certain sectors such as energy, communications, finance, water supply, emergency services, etc. It is important to note that the law does not explicitly state that any infrastructure must be labeled as critical, but that any infrastructure that meets the criteria may be included in the list, regardless of the form of ownership or, as an implication, (in)dependence of the government.

Considering that the CEC is an independent institution, the CEC may need to formally request to be designated as CI. Since some substantial changes in the IT structure would need to be put in place if the CEC is defined as CI, this will likely need to be regulated by a CEC decision. Some interlocutors understand that the CEC will sign a Memorandum of Understanding with the State Service for Special Communications and Information Protection (SSSCIP). They are one of the pillars of cybersecurity in Ukraine, and should not only designate the CEC a CI, but also any MoU should contain details about the way in which the SSSCIP would assist the CEC, considering the legal obligations that the SSSCIP has if an institution is listed as CI. According to CEC representatives, however, the de-facto cooperation with the security agencies providing cybersecurity services is often established just before elections, and such is foreseen again. According to the CEC, whether they are listed as CI or not, will influence certain important aspects; for example, it may lead to allocation of additional budgetary means for cybersecurity.

It would be beneficial to establish the timing and format for any such agreement between the CEC and the SSSCIP. It would also be important to know what level of detail such an agreement would include, and if the text of the agreement would be made public.

Importantly, the Law on Cybersecurity mandates the Cabinet of Ministers to issue detailed normative acts to supplement the law itself, including the procedures for assigning institutions as CI and requirements for audits. The government has a deadline of three months after the law came into force (i.e. 9 August 2018) to issue such acts. Some work has been already done in this respect; for example, there is an existing draft on security audits of the CI systems. However, it is unclear if the government is prioritizing this activity. Some interlocutors expressed their doubts, as they haven’t seen much consultation on the issue within the cybersecurity community in Ukraine.

14 In relation to banking systems only, these tasks fall under the responsibility of the National Bank.
Cybersecurity Infrastructure in Ukraine

Cybersecurity as a component of national security is carried out by the president, through the Council of National Security and Defense, which the president heads. A body within this council, the National Cybersecurity Coordination Center, maintains the Cybersecurity Strategy of Ukraine.

The main agencies in the national system of cyber security are the SSSCIP, the SSU, the Cybercrime Unit within Police, the Ministry of Defense, and intelligence agencies.

NATO explained to the assessment team that the first stage of inter-institutional assistance has been provided, through a NATO cyber-defense trust fund, led by Romania. NATO provided significant assistance in equipment and training in building up Security Operation Centers (SOC) in both the SSU and SSSCIP. The SOCs provide services to government and other critical entities such as threat detection and mitigation. Having two SOCs allows for a redundant approach in relation to the detection of cyber threats. On the other hand, according to the Law on Cybersecurity, all cybersecurity activities are coordinated by the National Cybersecurity Coordination Center.15 Both centers use sensor architecture, which consists of hardware and software sensors (agents) needed to be placed in CI objects.

Certain government networks are included in the SSSCIP security perimeter and the CEC is currently not included in it. There are several benefits in case an institution’s network is considered CI, including: installation of sensors within such networks to monitor, inspect and log all traffic, penetration tests on components, and incident response through the CERT-UA (CERT-UA is part of SSSCIP). The new legislation provides that all institutions classed as CI must be protected by the SSSCIP.

According to the SSSCIP, it is not yet clear if the CEC will be part of SSSCIP’s secure perimeter. However, regardless of this, the SSSCIP is already in agreement with the CEC to install such sensors (hardware and software). It is important that the agreement related to the status of the CEC is determined as soon as possible to avoid lack of clarity on responsibilities and accountability. The CEC wants the SSSCIP to have more responsibility in securing the election networks. SSSCIP collaborated previously with the CEC at the time of elections (around 10 days before elections and after), through installing temporary sensors and embedding one technician to monitor the traffic and health of the Results Management System (RMS).

The SSU coordinates all collaboration with NATO and Ukrainian institutions on cybersecurity, including any potential assistance of NATO to the CEC. Among others, SSU undertakes operational activities to combat cyberespionage and perform spot checks of CI facilities for readiness against cyberattacks.16

---

15 This center is the working body of the National Security and Defense Council of Ukraine, headed by the President of Ukraine.
16 In other words, it appears that the SSU has a legal license to conduct audits without giving notice.
Cybersecurity and the Election Administration

There are three main components to the CEC’s IT system. First, the State Voter Register (SVR) is continuously operational and separate from the rest of the CEC’s IT system. A total of 700 locations around Ukraine are used as data entry points to update the SVR, and a total of 2,000 officials are operating the input and other systems. The system is entirely disconnected from the Internet, using an intranet owned by the state, although this fact may not protect it against cyberattacks. The data contained within the SVR is based on paper records maintained at the base institutions (local government offices). Among others, the CEC provided information to the assessment team on physical security of servers and possibilities for backend access, monitoring of the systems and sharing of secrets (passwords).

At present, the CEC does not have a formalized set of instruments for conducting a comprehensive security analysis in relation to system design and implementation, detailing all security assumptions. The CEC sees the threat of an insider attack on the central level as the only possible malware input vector in terms of security of the SVR. However, it said that by far the biggest danger in the electoral sense in terms of accuracy of the voter registers is the perception of the electorate that the lists are not correct; typically, a belief that there are deceased voters still present that others are voting on behalf of.

The second element is the relatively static system of information that is included on the CEC website (internet-facing part of the system) as well as the CEC intranet, emails system, etc. The third main component is the RMS, which is partly or significantly redesigned before every election.

Recently, the CEC has designed a program for replacing outdated equipment. This process is very important, since certain outdated components can be dangerous to use, due to discontinued support from the vendor and accumulation of identified security vulnerabilities in the hardware (both disclosed and potentially undisclosed).

Initially, the CEC created a general list of items they wish to install in their IT systems. Both NATO and OSCE PCU offered assistance in purchase of significant parts of the equipment, while the CEC also plans to buy a small amount of equipment from their own budget.

Although it appears that the lists of equipment to purchase have been clarified both by the OSCE and by NATO, the procurement procedure has not yet started, except for the equipment from the OSCE dedicated for the State Voter Register systems maintained within the CEC.

---

17 In Ukraine, the threat of an insider attack is considered seriously, due to cultural, lingual and physical proximity of the likely adversaries, as well as the stakes involved, especially in elections.

18 The reason for such redesign of the RMS architecture is the need to implement variations in operational requirements from election to election, a possible change of subcontractor and, as a result, a need to implement new set of security features.
This can potentially become problematic, having in mind that the procurement procedures might be quite cumbersome and that a substantial amount of work must be done with newly purchased equipment before the 2019 elections if the equipment is to be used. SSU representatives told the assessment team that they want the system components to be purchased by the end of August to allow for sufficient time for all other preparation.\textsuperscript{19} Representatives of the NATO Liaison Office expressed doubt that the procurement procedures, if any are initiated with NATO’s support will be conducive to meeting this deadline.

The OSCE initially considered providing advice on cybersecurity, but has declined to pursue this now due to mandate issues. Instead, they have budgeted for IT procurement and request a list from the CEC of what they need. Half of the budget for procurement of hardware and software is foreseen for the State Voter Register and half for the CEC IT department (total budget around 600,000 USD).

The main interest of the OSCE PCU in providing equipment is to increase the transparency of the election process, for example, by procuring a conference system to allow for online meetings and installing some workstations within the CEC to allow party proxies access to documentation that is not provided online. According to the OSCE PCU, this would help the CEC to address some outstanding OSCE/ODIHR recommendations. The OSCE also mentioned to the assessment team that the additional equipment for the “electronic workload system” will make documents more accessible to the public through greater capacity and better organization.

In case any new equipment is used in the next elections several important conditions should be met. First, it needs to be properly set-up and configured to ensure that there are no vulnerabilities. According to the SSU, NATO will not only provide the equipment, but also assist with set-up. The configuration of the system should be properly documented as well as the architectural design.

It would be useful to establish more precisely the timeline of acquisition of new equipment. More information about which equipment exactly is purchased would be of use, having in mind that further assistance to the CEC related with configuration and usage of some of the devices might be required. The CEC said they may require additional training on new equipment, but that at present they are not in position to define what that might be.

Any new equipment that is acquired by the CEC needs to be installed, set-up and properly configured. In addition, it needs to programmatically become an integral part of the pre-designed system architecture. If some newly purchased component (for example the network router) is misconfigured (can be due to lack of knowledge or haste), it may render the system much less secure and trivial to penetrate than before.

\textsuperscript{19}This deadline is not formalized anywhere according to the information that the pre-assessment team has.
The CEC faces an issue of trust from stakeholders stemming from problems experienced in previous election cycles. The mandate of 13 of 15 CEC members has expired and a new CEC should be appointed. A proposed list for candidates was sent by the president to the parliament, however, the issue has not been put on the agenda and it is unlikely to be resolved by the end of summer. The expectation of the change of the CEC composition reduces the effectiveness of its mandate, including in reaching decisions on future projects.

Presently, the CEC does not know their budget to prepare for next year’s elections. The CEC should propose a draft budget as early as possible, so that it can be included in the general budget draft by mid-September.

According to most of interlocutors, including the OSCE PCU and other available reports, the biggest problem that the CEC faces is a lack of human resources. The compensation for IT specialists is not sufficient compared to the private sector, to keep high quality workers on board. The CEC did not have capacity to produce terms of reference for their own website, which is currently being built with support from IFES.

According to the SSSCIP, the CEC IT system is complex and highly distributed, making it more difficult to protect all elements. The IT company that is currently designing the pilot Results Management System explained to the assessment team that the complexity is increased dramatically due to its architecture containing redundant systems for cyber-defense.  

Several interlocutors amongst which the SSSCIP and the OSCE PCU stated the importance of training of the CEC staff. The SSSCIP has a mandate to conduct such trainings. Both advanced trainings and trainings for beginners could be considered (for example training on basic cyber-hygiene for non-IT staff at the CEC). A training curriculum could be developed and proposed to the CEC. The OSCE specifically mentioned a need for training on maintenance of MS Windows systems related to cybersecurity.

The Results Management System (RMS)

The CEC explained to the assessment team that they are trying to modernize the RMS to have faster publication of preliminary results. Other goals are to increase internal integrity of the data in the results protocols through automation, and avoid issues of unrecorded changes to the protocols, especially at the District Election Commissions (DECs), and before they reach the CEC and the public. The CEC is attempting to encourage legislation to provide for pilot projects in this respect, but it seems it is currently unable to secure a sponsor for the draft (the CEC does not have the power of legislative initiative).  

---

20 For example, the results reporting system (internet-facing) is distributed to on multiple servers to tackle potential DDoS attacks.
21 The draft is publicly available in the Ukrainian language at: http://zakon3.rada.gov.ua/laws/show/v0273359-17
At present, the preliminary results are transmitted on paper from PECs to the DECs, where they are typed-up and sent over secure (isolated) lines to the CEC results server.\textsuperscript{22}

The main obstacle to introducing the new RMS remains the identification of users. According to the proposed design, biometric ID cards should be issued to all PEC members. These ID cards would provide both authentication of the sender, and encryption of information that has been sent (to prevent man-in-the-middle attack). However, this technology is not mature and is not widely used.\textsuperscript{23} Therefore, there would be a need to produce tens of thousands of such ID cards which would only be needed for elections. The capacity of production of ID cards can be increased by purchasing additional specialized printers. However, there is also an issue of distribution of the cards, especially since there is traditionally a high rate of replacement of PEC members just before elections.

The currently proposed solution foresees an MS Windows-based tablet with detachable keyboard that can connect to the Internet through a wireless connection, a smartcard reader and a printer. After authentication, the PEC members would be able to enter data into the PEC protocol electronically. The software contains redundancy reconciliation checks (i.e., whether protocols add up). PEC members would sign the protocols with their digital signatures. The protocol would then be dispatched to a central server, bypassing the DECs.

A solution that does not require digital signing of PEC protocol to ensure integrity could be considered, as long as the data is sent through encrypted channels. Access to the data entry system could be password protected or the data could be entered directly, through a web-browser. In this case, however, exchange of certificates should be carefully reviewed to avoid man-in-the-middle attacks, since not all network nodes are fully controlled and due to wireless connectivity of terminal devices in polling stations.\textsuperscript{24}

Apart from the issue of production and distribution of smart cards, another weak point is the potential for a DDoS attack on the collection server, since it has to be open to the Internet.

\textsuperscript{22} Results are copied to an internet-facing server for publishing them.

\textsuperscript{23} Previous technical issues include some problems with certification servers as well as using a third-party cloud outside of Ukraine (Amazon cloud).

\textsuperscript{24} Wireless connectivity is inherently insecure and can be attacked in numerous ways including, for example, through setting up fake access points with same name of a network identifier.
Cybersecurity and Election Audits

At present, Ukraine does not have a fully implemented cybersecurity framework and it uses the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) for security evaluation. However, according to the SSSCIP, the normative acts foreseen to be adopted by the Cabinet of Ministers will provide for the obligation to use ISO/IEC 27000 family of information security standards, the use of which is voluntary now.25

The NIST cybersecurity framework has also been translated into Ukrainian.26 It is yet unclear if the NIST framework will be used in any form in Ukraine.

The SSSCIP is mandated by the new Law on Cybersecurity to conduct cybersecurity audits for facilities and institutions that are listed as CI. The Cabinet of Ministers must pass a detailed act to ensure that there is a cybersecurity audit conducted for all facilities listed as CI. Arguably, the main element of such an audit is to conduct penetration tests, commonly referred to as pen tests.

Most interlocutors underlined the need for pen tests on the election systems. The CEC, however, is wary of such tests since if vulnerabilities are identified, they will have an unforeseen need for expenditure of resources, which may come at a bad time (i.e. very close to elections).

An important question is if the pen test on systems in the CEC will be conducted with due diligence. Interlocutors suggested anywhere from 10 days to a month for the conduct of pen tests. The cost of such tests was assessed by some interlocutors from the commercial sector to start from 10,000 USD. Problems with testing might also include the timing. The CEC tends to modify the system architecture before each election, due to operational needs; therefore, thorough tests should be conducted after this period.27 However, modification of the system design late in the process may present its own security vulnerabilities. Other means such as, for example, establishing a comprehensive cybersecurity strategy to be used when implementing any system changes could be an alternative. At present, the CEC does not have its own comprehensive cybersecurity strategy and formalized instruments to conduct cybersecurity reviews or audits, and a formal mechanism to address recommendations.

27 This excludes the State Voter Register which is constantly operational.
A cyberattack against Ukrainian elections can threaten not only the availability of the IT systems necessary to run the election, but also the credibility of the election results themselves. In conversations with interlocutors, the assessment team learned that a focus of the concern has been to guarantee the availability of the system. However, as part of this report the assessment team wanted to emphasize that the credibility of the result (namely, that it is not altered through a cyberattack) is equally important, as it creates trust in the absence of a cyberattack that the official result really reflects the will of voters.

One way to inculcate such trust is to conduct post-election audits (for example, risk-limiting audits) for the election where statistical evidence is collected to support (beyond a certain level of doubt) that the result is indeed correct. The introduction of such measures by the Ukrainian authorities could be an important step in this direction.
Recommendations

During the assessment, the team discussed initial recommendations in terms of cybersecurity in Ukrainian elections with key stakeholders, including with the CEC. A series of key short-term and long-term recommendations have been identified. Through this assessment, IFES extended its readiness to continue providing electoral assistance in Ukraine, including through new efforts to strengthen electoral cybersecurity.

Short-Term Recommendations:

R1. **Trainings on cybersecurity should be provided for various participants of the election process.** General staff (non-IT) in the CEC and DECs, including the members (and potentially new CEC members) should be explained the cybersecurity vulnerabilities and threats and trained on how to deal with cyberattacks. A practical tabletop exercise in this respect could be organized. A training curriculum could be developed and used for trainings in cyber-hygiene, but also for more targeted/specific lessons.

R2. **Increasing the capacity of the key IT personnel in the CEC** through providing more resources and targeted trainings related, for example, to configuration of new equipment.

R3. **Increasing cybersecurity awareness** of the employees in the election administration, including commission members and other staff. A more general course in cyber-hygiene would benefit all participants in the process.

R4. **Identify outdated hardware that must be replaced.** Outdated components may potentially be exploited and used to gain illegal access to the CEC networks. However, new components to be included in the system architecture must be procured sufficiently early for them to be properly configured and tested and so that personnel could be trained to operate it without introducing new and possibly undetected cybersecurity vulnerabilities.

Long-Term Recommendations:

R5. **Increase collaboration with state security agencies** and other relevant election stakeholders in order to increase operational resilience, monitoring capacity and mitigating threats.

R6. **The CEC, could consider developing a comprehensive cybersecurity strategy.** This could be done in collaboration with other institutions, primarily the SSSCIP. This strategy could include detailed guidelines on how to identify threats, protect the systems, detect intrusions, respond to attacks and restore in case of successful attack.
R7. **Consider conducting a post-election audit.** Post-election audits comprise random mandatory partial recounts to establish the accuracy and integrity of election results. It is increasingly used in various jurisdictions as a risk-mitigation strategy as well as a way to increase confidence in election results by the electorate. While post-election audits are paramount for elections with an electronic vote-count (for examples, by ballot box scanners), it is a good practice to consider it also for elections in which vote-count is conducted by human operators. The introduction of this type of audit requires changes to election legislation, but also political will to tackle the issue of accuracy of election results.
Annex I: Meetings on cybersecurity with key stakeholders

May 14-18, 2018

- **Central Election Commission of Ukraine** – Zhanna Usenko-Chorna, Deputy Head, Valerii Striganov, Head of the CEC Department of Informatization, Oleksandr Stelmakh, Head of the State Register of Voters, Andrii Versal, Deputy Head of the State Register of Voters

- **State Service for Special Communication and Information Protection (SSSCIP)** - Roman Boiarchuk, Director of the State Center for Cyber protection and Counteraction to Cyber Threats

- **The Presidential Administration of Ukraine** - Dmytro Shymkiv, Deputy Head, National Reforms Council Secretary

- **Security Service of Ukraine** – Maksym Litvinov, Head of the Situational Center for Cyber Security

- **OSCE Project Co-ordinator in Ukraine** - Yevhen Poberezhnyi, Election and Governance Advisor, Ihor Tkachenko, Elections Officer

- **Medirent IT Company** – Oleksii Bondarchuk, Deputy Head, representatives of different departments

- **Berezha Security** (Ukrainian cyber-security company focused on Offensive Security and Security Awareness) - Kostiantyn Korsun, Executive Director

- **CYS-Centrum** – Mykola Koval, Director

June 4-8, 2018

- **Central Election Commission of Ukraine** – Serhii Dubovyk, Deputy Head of the Secretariat, Valerii Striganov, Head of the CEC Department of Informatization, Andrii Versal, Deputy Head of the State Register of Voters

- **NATO Representation to Ukraine** – Aleksander Vinnikov, Head of Representation, Director, NLO, Béla Téczely, Lieutenant Colonel HUN AF, C4I Advisor, Acting Cyber Defence Advisor

- **EU Delegation** – Tanel Tang, European Commission Directorate General Neighbourhood and Enlargement Negotiations, Rikard Barkeling, Political Section, Marco Ferraro, Operations Section

- **OPORA Civic network** – Yurii Lissovskyi, IT Expert
Annex II: Program of the Expert Round Table
“Cyber Threats for the Electoral Process in Ukraine”

June 7, 2018
Radisson Blu Hotel (22 Yaroslaviv Val)

13:30 - 14:00 Registration and Welcome Coffee

14:00 - 14:15 Welcoming Remarks

Moderator: Yuliya Shypilova, Senior Electoral Advisor, International Foundation for Electoral Systems

- Mykhailo Okhendovskiy, Chairman, Central Election Commission of Ukraine
- Dr. Beata Martin-Rozumilowicz, Regional Director for Europe and Eurasia, International Foundation for Electoral Systems

14:15 - 15:15 Cybersecurity Challenges for the Central Election Commission of Ukraine Ahead of the Elections in 2019

Moderator: Yuliya Shypilova, Senior Electoral Advisor, International Foundation for Electoral Systems

Speakers:
- Dr. Beata Martin-Rozumilowicz, Regional Director for Europe and Eurasia, International Foundation for Electoral Systems
- Valerii Striganov, Head, Department of Informatization, Central Election Commission of Ukraine
- Roman Boyarchuk, Head, Center for Cyber Protection, State Service for Special Communication and Information Protection
- Victor Zhora, Cyber Security Expert, CEO, InfoSafe IT

Moderated discussion

15:15 – 15:45 Coffee Break

15:45 – 16:45 Coordination of Stakeholder Efforts in Countering Cyber Threats

Moderator: Yuliya Shypilova, Senior Electoral Advisor, International Foundation for Electoral Systems

Speakers:
- Konrad Olszewski, Project Director, EU Election Observation and Democracy Support (EODS) project
- Maksym Litvinov, Head, Cybersecurity Coordination Center, Security Service of Ukraine
- Carsten Schürmann, Associate Professor, Centre of Information Security Research, IT University of Copenhagen
- Yevhen Poberezhnyi, Election and Governance Advisor, OSCE Project Co-ordinator in Ukraine

Moderated discussion

16:45 - 17:00 Closing Remarks
Annex III: List of participants of the Expert Round Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization and position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barkeling Rikard</td>
<td>EU Delegation, Political Section</td>
</tr>
<tr>
<td>Boiarchuk Roman</td>
<td>State Service for Special Communication and Information Protection (SSSCIP), Director of the State Center for Cyber protection and Counteraction to Cyber Threats</td>
</tr>
<tr>
<td>Bondarchuk Oleksii</td>
<td>Medirent IT Company, Deputy Head</td>
</tr>
<tr>
<td>Darkin Maksym</td>
<td>Project Management Specialist (eGov), Office of Democracy and Governance USAID Ukraine</td>
</tr>
<tr>
<td>Dubok Hennadiy</td>
<td>National Police of Ukraine, Deputy Head of the Department of the Cyber Police</td>
</tr>
<tr>
<td>Erben Peter</td>
<td>Senior Country Director, IFES Ukraine IFES Senior Global Electoral Advisor</td>
</tr>
<tr>
<td>Koval Mykola</td>
<td>CYS-Centrum, Director</td>
</tr>
<tr>
<td>Kuleshov Mykola</td>
<td>Security Service of Ukraine</td>
</tr>
<tr>
<td>Kyrchenko Yuliy</td>
<td>Center for Political and Legal Reform (CPLR)</td>
</tr>
<tr>
<td>Litvinov Maksym</td>
<td>Security Service of Ukraine, Head of the Situational Center for Cyber Security</td>
</tr>
<tr>
<td>Mahea Andrii</td>
<td>Central Election Commission, Deputy Head</td>
</tr>
<tr>
<td>Ferraro Marco</td>
<td>EU Delegation, Operations Section</td>
</tr>
<tr>
<td>Martin-Rozumilowicz Beata</td>
<td>IFES, Regional Director for Europe and Eurasia</td>
</tr>
<tr>
<td>Okhendovskiy Mykhailo</td>
<td>Central Election Commission, Chairperson</td>
</tr>
<tr>
<td>Olasiuk Natalia</td>
<td>IFES, Project Officer</td>
</tr>
<tr>
<td>Olzowski Konrad</td>
<td>EU Election Observation and Democracy Support (EODS) project, Project Director</td>
</tr>
<tr>
<td>Petrov Goran</td>
<td>IFES, Cyber Security Expert</td>
</tr>
<tr>
<td>Pobereznyi Yevhen</td>
<td>OSCE Project Co-ordinator in Ukraine, Election and Governance Advisor</td>
</tr>
<tr>
<td>Schmidt Juliette</td>
<td>IFES, Senior Elections, Political Processes &amp; Security Specialist</td>
</tr>
<tr>
<td>Schürmann Carsten</td>
<td>Associate Professor, Centre of Information Security Research, IT University of Copenhagen</td>
</tr>
<tr>
<td>Shypilova Yuliya</td>
<td>IFES, Senior Electoral Advisor</td>
</tr>
<tr>
<td>Smolina Iryna</td>
<td>USAID/Ukraine, Office of Democracy and Governance, Project Management (Democracy, Rights &amp; Governance) Specialist</td>
</tr>
<tr>
<td>Smyrnyov Konstantyn</td>
<td>Security Service of Ukraine</td>
</tr>
<tr>
<td>Striganov Valerii</td>
<td>Central Election Commission, Head of the Department of Informatization</td>
</tr>
<tr>
<td>Tang Tanel</td>
<td>European Commission Directorate General Neighbourhood and Enlargement Negotiations</td>
</tr>
<tr>
<td>Téczely Béla</td>
<td>Lieutenant Colonel HUN AF, C4I Advisor, Acting Cyber Defence Advisor</td>
</tr>
<tr>
<td>Versal Andrii</td>
<td>Deputy Head of the State Register of Voters</td>
</tr>
<tr>
<td>Zahrebelnyi Serhii</td>
<td>Security Service of Ukraine</td>
</tr>
<tr>
<td>Zhora Victor</td>
<td>Cyber Security Expert, CEO, InfoSafe IT</td>
</tr>
</tbody>
</table>