Cybersecurity in Ukrainian Elections

A Cybersecurity Playbook

Combating Threats to Ukrainian Elections through Good Practice

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
· 30 Years ·

A Cybersecurity Playbook

Combating Threats to Ukrainian Elections through Good Practice

November 2018

Authors:

Goran Petrov and Thomas Chanussot

Contributors/Editors:

Victor Zhora, Giorgi Iashvili,
Katherine Ellena and Juliette Schmidt

This publication was prepared 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.

A Cybersecurity Playbook Combatting Threats to Ukrainian Elections through Good Practice

International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
E-mail: editor@ifes.org
Fax: 202.350.6701

Contents

The Role of IFES: Cybersecurity in Elections

About Us

Since 1987, the International Foundation for Electoral Systems (IFES) has worked in over 135 countries to support citizens' right to participate in genuine and democratic elections. IFES' independent expertise strengthens electoral systems and builds local capacity to deliver sustainable solutions.

Since 1994, IFES has played a key role in the emergence of democratic electoral processes and institutions in Ukraine. IFES has developed a reputation as a reliable source for impartial analysis and high-quality technical assistance in the fields of electoral and political finance law reform, election administration, civil society capacity building and public opinion research. Currently, IFES is implementing the following projects in Ukraine: (1) the Ukraine Responsive and Accountable Politics Program, funded by the United States Agency for International Development, and (2) Electoral and Legal Enhancements through Civic Engagement and Technical Assistance Program, funded by UK aid.

Current and Future Assistance in Cybersecurity in Elections

Cybersecurity has a significant influence on the stability of Ukraine particularly in elections. IFES currently supports the Central Election Commission of Ukraine (CEC) to strengthen its cybersecurity efforts. In June 2018, IFES conducted an Assessment of the Cybersecurity in Ukrainian Elections with input from election and government stakeholders in cybersecurity and elections, as well as civil society and commercial vendors. The assessment yielded an initial set of short-term and long-term recommendations for the CEC, considering that both presidential and parliamentary elections are scheduled for 2019.

IFES continues to support electoral stakeholders on cybersecurity issues pertaining to the the Ukrainian elections. Activities include:

Technical Support: IFES shares good practices and recommendations with the CEC and other election stakeholders in Ukraine, including through this playbook.

Facilitation of Key Stakeholder Coordination: IFES supports the CEC to engage with other electoral stakeholders to facilitate information exchange through informal expert roundtables, conferences and other events for cybersecurity and election professionals. Also, IFES has founded a cybersecurity and elections working group and shares accumulated resources in English and in Ukrainian.

Cybersecurity Crisis Simulations: IFES developed and conducted a cybersecurity crisis simulation in November 2018 to improve the CEC's crisis leadership, to assist in preparation and planning for cyber crises during the electoral cycle.

Interactive Cyber Hygiene Training: IFES developed an Interactive Cyber Hygiene course for CEC members, staff and other non-IT professionals working in elections, drawing on its vast experience in interactive courses, including the Building Resources in Democracy, Governance and Elections (BRIDGE) project. IFES conducts the trainings through its network of experienced trainers.

CEC and State Voter Register (SVR) IT Staff Training: IFES, in collaboration with the CEC has organized a series of trainings in system information security, network security, and security audit practices, to bolster CEC IT specialists dealing with possible emerging cybersecurity issues.

International expertise and study trips: IFES provides specialists from around the world to share relevant knowledge and experience in Ukraine and through international study trips, providing for a comparative approach and distilled good practices.

Introduction

Elections around the world face diverse and increasing threats. In Ukraine, some threats are well known and include both the potential of black-hat hacker attacks from within the country as well as known foreign Advanced Persistent Threats (APTs) which attempt to gain and maintain unauthorized access to a computer network for prolonged periods of time. Examples of APT groups include APT28 or Fancy Bear, and APT29 also known as Cozy Bear. APT28 is thought to be behind the attack on the CEC Ukraine infrastructure in 2014. Others are less known, but can be equally damaging to a democratic electoral process.

Purpose of This Playbook

Cybersecurity in general has received considerable attention in recent years, however, cybersecurity in the elections field had been seriously neglected at a time in which countries have started introducing technology in their election processes in earnest. This playbook draws from the emerging knowledge-base in the U.S. and in Europe, as well as IFES experience globally, in order to present good practices. It also presents the most common threats in order to raise awareness about associated risks.

This playbook is not intended to be a comprehensive technical document. Most information in the text requires only basic understanding of IT but some level of understanding of the dangers associated with disruption of election processes.

The text provides an overview of issues relevant to cybersecurity in Ukraine's electoral system and protection of the election infrastructure in light of international good practice. The playbook applies a holistic approach developed by IFES to mitigate cybersecurity risks and offers both general (high-level) as well as more detailed (technical) recommendations on short-term and long-term improvements.

This playbook is not an attempt to provide a complete overview of all problems associated with cybersecurity at the time of elections. For example, the subject of disinformation during the campaign period is not considered as it does not fall under the direct purview of most EMBs, including the CEC of Ukraine, with the exception of addressing disinformation surrounding the electoral process i.

Many issues presented here are well known to the CEC's IT experts who are also responsible for the cybersecurity of distinct systems: the State Voter Register, Results Management System and digital workload system. We hope that these experts will find this text useful as they continue their serious efforts to safeguard the Ukrainian elections.

This playbook is a living document. For comments and corrections, please contact secureelectionsua@ifesukraine.org.

Who This Playbook Is For

First and foremost, this text is intended for Ukrainian CEC members and Secretariat, both IT specialists and non-IT staff. It may also be useful for District Election Commission (DEC) and Precinct Election Commission (PEC) members, and other election stakeholders closely involved in cybersecurity, such as government, political parties or civil society.

Cybersecurity of Elections

Digital information and interconnectivity over the Internet have accelerated communications and allowed economies of scale, but they have also introduced new threats to critical infrastructure. This digitalization increases the complexity of information systems and creates new and more complicated ways to exploit them. The potential for adversarial and destructive activity also increases significantly.

Election systems are no exception, regardless of whether ballots are cast and counted by hand or by machine. Even if EMBs are skeptical of introducing electronic voting, most EMBs in the world use digital systems in some capacity while administering elections, starting with voter registration and finishing with electronic publication of election results.

In the context of the Ukrainian presidential and parliamentary elections in 2019, cyber-attacks are a real and present danger.

An election in which there is doubt that the will of voters fairly translated into elected mandates leaves a wound that is difficult to heal. Cyber attacks have the potential not only to compromise an election process, but to create doubt and uncertainty about the integrity of an election. This is true if they occur on their own, but especially if they occur in conjunction with any other perceived irregularities, controversies or disputes. In Ukraine, Russia's occupation of Crimea and the conflict in Eastern Ukraine has clear characteristics of hybrid warfare - combining traditional and cyber tactics with other methods of warfare. With Ukraine's 2019 presidential and parliamentary elections approaching, the prospect of cyberattacks that could undermine critical systems could have severe ramifications for country.

CEC as Critical Infrastructure (CI)

The relatively new Law on Cybersecurity in Ukraine (in force since May 2018) establishes a possibility for the government to designate specific infrastructure as critical infrastructure (CI). Though the government has not yet approved the list of critical infrastructure, the CEC systems are already de facto CI. Until now, the practice has been for the State Service of Special Communication and Information Protection of Ukraine (SSSCIP) and the Security Service of Ukraine (SSU) to be embedded in the CEC for several days around Election Day to help with both network protection and general information security. The CEC would benefit from formalization of that process as it would prescribe what resources the CEC can rely upon from the government in a transparent manner, ascertaining its independence towards other agencies, while also pinning down who is responsible and accountable for what.

Layers of protection by the SSSCIP:
Inner-most government systems (CERT-UA-protected)
Other state bodies (the rest of the government)
Public Critical Infrastructure (CI sensors)
Privately-owned Critical Infrastructure (CI sensors)

Who is Responsible for Securing the Elections Against Adversaries?

Election Management Bodies (EMBs) around the world are responsible for administering genuine, inclusive, democratic elections that represent the will of the people. While there are often a number of government entities responsible for election security, including cybersecurity, in the court of public opinion it is often the EMB that is perceived as responsible for providing a safe environment for elections. In Ukraine, as in most countries, elections are administered by a permanent, centralized

Election Management Body (EMB) on top of a structure, typically district and local-level election commissions. Ukraine's CEC is a formally independent body.

In addition, where the EMB owns specific parts of the electoral IT infrastructure, such as the voter register, there is an emerging consensus that they also have the responsibility to protect such data. While not enshrined in case law, punitive measures imposed on the EMB in the Philippines in 2016 are instructive in terms of the EMB's responsibility for cybersecurity in elections. In March 2016, the Philippines Commission on Elections (COMELEC) was hacked by a group called Anonymous Philippines. The hackers took over COMELEC's website and released extensive voter information, including fingerprints. The National Privacy Commission also recommended criminal charges against COMELEC Chairperson Andres Bautista for negligence. This case is a compelling example of potential institutional and personal liability for EMBs and election officials with respect to cybersecurity in elections. The Ukrainian CEC has the overall responsibility for maintaining the voter register as well as for all other election systems and activities.

While the CEC has both the legal and de facto responsibility to ensure the cybersecurity of its systems, it is assisted during the election period by the SSSCIP, the SSU, the National Police, the National Security Defense Council of Ukraine, the Ministry of Defense and the Foreign Intelligence Service. Typically, this help consists of providing and operating sensors for alerts and warnings, but also coordination in case of incidents.

> The national cybersecurity system in Ukraine consists of the National Security and Defense Council of Ukraine, the SSSCIP, the SSU, the National Police, the Ministry of Defense and the Foreign Intelligence Service.

Maintaining the independence of the Ukrainian CEC, and isolating any negative external influence, both real and perceived, is crucial. Therefore, it is of utmost importance to both the integrity of elections and the trust of citizens in the process, that the nature and the scope of any assistance is transparent and that formal inter-institutional collaboration takes place to detect, prevent and respond to threats.

IFES' Holistic Approach to Cybersecurity in Elections (The HEAT Approach)

To be protected against cyber-attacks, it takes an interdisciplinary approach, and an understanding of potential threat vectors. A breach of a Facebook account of a politician, for example, may lead to serious issues on seemingly unrelated topics, such as, a decline in trust of election stakeholders in the integrity of the State Voter Register.

IFES has developed a methodology to consider and mitigate and/or prevent threats to cybersecurity using a method called Holistic Exposure and Adaptation Testing (HEAT). The purpose of the HEAT approach is to differentiate and understand the five types of exposure to potential threats: technology, human, political, legal and procedural. Each of these is considered separately and in concert using a five-step functional approach: Identify, collect, expose, exploit and adapt.

More information about IFES's HEAT methodology is included in the Appendix. A full overview is available on the IFES website.

The Ukrainian Election Infrastructure

Facing the election season in 2019

Persistent threats to cybersecurity in conjunction with the vulnerabilities in the election system will pose a risk in the upcoming presidential and parliamentary elections scheduled for March 31 and October 27, 2019, respectively.

Efforts have been made to improve the security of critical infrastructure, and protection of election systems against such attacks has been a recurrent topic within the cyber community in Ukraine. The CEC has introduced several cybersecurity improvements since experiencing a significant cyber attack on its digital infrastructure on the eve of the 22 May 2014 early presidential election. Among these efforts to improve the cybersecurity posture of the organization, the CEC has segmented the office network (the workload network) and critical networks, a modern and comprehensive network monitoring system has been installed, partly owing to its collaboration with the government security agencies. It is also replacing outdated critical network equipment, and upgrading major system hardware and software components (public facing website, servers, network equipment). The CEC is also a lot more aware of the risk that cyberattacks represent to the elections, all the secretariat staff have received a cyber security hygiene training by the end of 2018.

This chapter attempts to describe the cybersecurity of elections and the need to protect election processes and the flow of election results data.

The CEC and Its Secretariat

As an independent institution, the CEC has an extensive mandate in preparing and overseeing the conduct of presidential and parliamentary elections. Its mandate in local elections is more limited. The CEC comprises 17 members who are appointed by the *Verhovna Rada* based on nomination of candidates by the President following consultations with political factions and groups. Currently, one of the 17 seats is vacant. All parliamentary factions but one are represented on the commission.

The renewal of the CEC in October 2018 opened the door to address some of the cybersecurity vulnerabilities, such as the lack of transparency in certain aspects of the election process.

The renewed CEC is already taking the cybersecurity of elections seriously. It has assigned a CEC member to deal specifically with this topic and has engaged in a number of activities, including training of both its IT and non-IT staff, with the support of IFES.

The CEC Secretariat is a professional body and consists of an experienced pool of highly qualified administrative staff members in continuous service to the CEC. It comprises approximately 250 employees working in 15 departments. The DEC (District Election Commissions) are temporary bodies, they are appointed 40 days before the presidential election and 62 days before the parliamentary election. The State Voter Register (SVR) Service is a separate organizational unit within the CEC and has four departments.

The State Voter Register (SVR)

The voter registration system in Ukraine

Voter lists are based on the State Voter Register (SVR), which is maintained at the central level by dedicated staff in a separate unit within the CEC. The registration process is passive, meaning that the authorities have a legal obligation to include all eligible Ukrainian citizens with the right to vote in the SVR.

In total, some 31 million voters are registered. The SVR is compiled by the CEC based on data from local government offices that issue identification cards and register changes in residence and civil status, such as marriages and deaths.

In terms of cybersecurity, the SVR is not under an immediate critical threat, largely due to the continuity of the system of paper-based voter lists in polling stations. The accuracy of the source data contained in the voter lists on election day, however, is an issue and deserves significant attention. For example, the municipal authorities who are in charge of deregistering and registering voters based on place of residence may fail to report the most updated information to the local offices of the state administration who, in turn, communicate with SVR staff to reflect changes in the voter register.

Design of the State Voter Register (SVR)

The SVR is updated electronically based on input provided by 27 Register Administration Bodies (RABs), and 761 Register Maintenance Bodies (RMBs) which are supervised by the CEC. RMBs are part of the state administration at the rayon level. All bodies located in the Autonomous Republic of Crimea and Sevastopol (33 in total) are inaccessible at present, due to the occupation of the Crimean Peninsula by Russia. In the east of the country, due to the conflict in the Donbas region, 32 of the 62 bodies in Donetsk oblast and 19 out of the 34 bodies in Luhansk oblast are not accessible at present.

The SVR is updated on a monthly basis. State and local institutions provide most data to the RMBs electronically.

The SVR regularly works to clean the voter register at the central level of the CEC, for example by removing duplicate entries (due to re-registration without de-registration). The CEC does not only host the voter register but also manages the voter list data directly.

Software and Configuration

The design of the SVR database and the front-end software, including the code of the data-entry system for RMBs, is developed in-house by a team at CEC's SVR Service. The SVR Service does not deal with external contracts and associated risks, but fully relies on its internal capacity with regards to support and maintenance.

At the CEC, dedicated lines are connected to a cluster of routers directing the traffic to the SVR server.

Access and Accountability

Due to the need for the SVR office to routinely access and handle election data, there is a risk of accidental or deliberate modification of data leading to a less accurate voter register. For example, maintenance of the voter list for duplicate entries requires the SVR Service resolve conflicting entries for individual voter by altering the data.

The State Voter Register Website

According to the SVR Office, a total of 200,000 voters have checked their data since 2013. Currently, the process for checking a voter's registration status online requires the pre-registration of an account. The accounts can be created using multiple services (facebook, google, BankID, etc), but can require 48 hours to be activated. This can be a deterrent for voters who want to do online checks. However, the website to review voter's detail is well design and users can access polling station information easily.

The internet-facing equipment, including servers that allow citizens to check their registration status, is separated from the main SVR network, in line with good practice. Hacking the website in the critical periods before election day, between the time of the publication of the preliminary and final voter lists, would not damage the SVR database itself. However, if such attacks prove successful, they can erode the trust in the security protection of the SVR system, especially if combined with disinformation campaign about the alleged associated damage. Subsequently, the trust in the integrity of the voter list may erode as well.

In August 2018, a hacker from an outfit known as the Ukrainian Cyber Alliance exposed a vulnerability in the SVR website and posted information about it on Facebook. The hacker discovered cross-site scripting (XSS) vulnerability that could potentially compromise users who access the CEC website (the result of such an attack could be theft of the private email login credentials of a CEC member). In addition, the hacker began to publicly question whether the SVR is sufficiently protected. A summary article on this topic was published in September 2018.

The CEC responded that the the vulnerability identified had no impact on the SVR main database as it is segregated from the associated websites. However, the public perception impact should not be downplayed.

Printing and Distribution of Voter Lists

The printing and dissemination of the voter register to the polling stations (the PEC-level voter lists) is a critical process that needs to be safeguarded. By law, preliminary voter lists (PVLs) are distributed to polling stations from more than a week to less than three weeks before election day, depending on the type of the election, while the final voter lists (FVLs) are delivered no later than two days before election day.

A delay in the delivery of preliminary voter lists to polling stations would impede the ability of voters to familiarize themselves with the lists, inquire where to go to vote and verify that they are included in the list at the correct polling station. A delay in the delivery of the final voter lists could negatively impact the election process, since election-day registration in polling stations is not permitted.

Integrity and Accuracy of the SVR

The CEC relies on the integrity of the central SVR database as a means to ensure that there is no loss of voter registration data. The CEC needs to be able to act quickly in case of cybersecurity incidents or accidental loss of data. Online and offline backups are created regularly and, if required, the system could be recreated from backup. Recovery from significant loss of data is not a simple process, a disaster recovery plan should be established and regularly reviewed, especially for such a critical database as the SVR. Since voter data changes constantly, a sophisticated approach including incremental and full backup for both online and offline repository is of utmost importance.

The Human Capacity to operate the SVR

Compensation for IT/cybersecurity work is considerably higher in the private sector, therefore it is difficult to retain qualified personnel in the public sector. In recent years, data shows a turnover rate of almost one-third of all IT personnel. The CEC and representatives of government security agencies have reiterated that the lack of sufficient human resources is a long-standing concern across all sectors of government.

While permanent data entry operators for the SVR, especially in the Registration Management Bodies, do not need to possess comprehensive skills on the operation and functionality of the SVR software, cyber hygiene and discipline to strictly adhere to security procedures set by the CEC are of great importance in order to prevent possible breaches.

Network connectivity

Registration Management Bodies are connected directly to the SVR office at the CEC using a fiber optic connection provided by UkrTelecom. The possibility of damaging the main network nodes in UkrTelecom by physical destruction could be considered. The National Police has been tasked by the Government to ensure the physical protection of these assets.

The Results Management System (RMS)

Characteristics of the RMS

The results consolidation and management processes that will be used in 2019 will be similar to the ones from 2014. The RMS database and software are designed anew for each election, using the previous elections' system designs. The design schematics and interconnectivity, as well as the inclusion and location of specific components, are upgraded or altered.

The primary component is the main database server to which DECs are directly connected.

Since DECs are temporary bodies, the DEC-level results system is not setup until the DECs are established prior to the election.

The Results Reporting System (RRS) is a part of the RMS, but segregated from the main RMS infrastructure. It is designed to be accessible via the Internet so the public can view the election results.

It is very important to keep in mind that the election results published on the CEC website during election night are preliminary results. The official results are those contained in the signed summary protocols. Therefore, if the RMS is compromised, that does not mean that the integrity of results would be compromised. A paper record of the results is present at each PEC (the PEC results protocol) and helps ensure the integrity of results. All electronic data is checked against the official paper records. However, a successful attack on the results system, depending on its severity, could have a negative impact on the election process by spreading confusion, uncertainty and doubt from electoral stakeholders about the results.

The CEC will rely on the SSSCIP to perform vulnerability tests, including pen tests on the RMS, following the practice that was established in previous elections.

Data-Entry of Results at the DECs

The CEC does not have a pool of hardware for DEC use during the data entry of results, as the DECs are not permanent institutions. The DECs generally use computers from local offices of the state administration. Situations in which privately-owned computers are used has occurred in previous elections. This may represent the biggest cybersecurity vulnerability for the RMS.

These computers are connected to the protected wider network of the RMS, but may not be fully controlled and it is possible that malware could be installed or the computers could be left unattended or not properly secured.

Results Reporting System (RRS)

The RRS is a distributed system placed in multiple physical locations and the results website is one of the most obvious targets for attack during the Ukrainian elections.

The peak time frame during which the reporting of the results is interesting to the broader public is very short, in all likelihood only a few hours during the election night, especially for the presidential election for which the result returns are fairly straightforward.

Snapshots of the results are taken from the internal protected RMS and copied to the external web server where the election results are hosted, on a regular basis.

The SSSCIP provides the network monitoring and intrusion sensors on the web server at the CEC. From thereon, the results are mirrored to multiple locations in Kyiv to fence off DDoS attacks. Public access to the website is routed to the mirrors transparently.

Age of hardware and software

Outdated hardware becomes a cybersecurity concern when vendors stop support. The routers used up until late 2018 within the CEC have been recognized as vulnerable by the vendor and are no longer supported. They could be exploited and used to gain illegal access to the CEC networks and compromise both the RMS and the SVR. The CEC is in the process of procuring replacement and upgrade for all outdated equipment with support from IFES. The timely installation and testing of this equipment is going to be critical to the protection of the systems that the CEC will use during the 2019 election.

Crisis Planning, Crisis Response

Creating a crisis response plan can feel overwhelming for an electoral management body, there are so many things to consider and they might not feel like they are having all the support they need.

However, as important as it is to establish cybersecurity defense, EMBs have to prepare for the worse, and expect that adversaries will find a way to disrupt the electoral process. To face this eventuality, EMBs have to carefully prepare and plan for how they will deal with cyber incident both internally and with the public.

1. Communication plan

The objective of the communication plan, and of the communication department at large during and after a cyber incident occurs, is to maintain public trust in the electoral process.

EMBs, particularly the communication departments need to have sufficient knowledge of the incident so they can educate the public about its nature and its impact.

As described later in this document, the balance between what can be told to the public and what should be kept secret to prevent adversaries to find ways to escalate the issue can sometimes be difficult to reach. However, based on previous experience, it is clear that everything that does not risk escalating the problem should be calmly explained to the public.

A communication plan should include publication strategy, to determine the roles and responsibilities inside the communication department and with the commissioners. It should contain response to cyber incident prepared in advance, based on previous cyber incidents and on recommendations from the IT department.

For more information about the preparation of coordination of cyber incident communication, refer to the Election Cyber Incident Communications Plan Template[1].

2. Contingency plan/Business Continuity plan

A business continuity plan can help ensure that election critical processes can continue during a time of emergency or disaster. While the focus here is on cyber incident, it should also go beyond and take into account a fire or any other hazard that could prevent the electoral process to function under normal conditions.

A business continuity plan involves looking at the organizational threats and establishing, if these materialize, what will be the list of the primary tasks required to keep the electoral operations flowing with minimal disruption. It could involve switching to a secondary data center if the main data center is attacked, or reverting to manual count and physical file transfer if there is a network disruption between a DEC and the CEC.

3. Recovery plan

Not to be mistaken with the Business Continuity plan, the disaster recovery plan refers to having the ability to restore the data and applications that run the election processes should data center, servers, or other key infrastructure be disrupted, damaged or destroyed.

The disaster recovery plan will detail the location of each backup storage and backup facility, as well as the processes to initiate the retrieval of the backup. These processes need to be regularly tested.

[1] https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template

An important consideration is the time it takes to recover data (downtime) as it can have a dramatic impact on the credibility of the electoral process.

The format of the response to a crisis, as it is defined in the crisis planning needs to be tested, rehearsed and understood by all stakeholders.

Technical simulations are the best tool available to ensure that the chain of command and the exchange of information is well understood:

- internally, it should involve the communication department, the IT department (or the agency who has the technical knowledge of the systems and infrastructure), but also any other relevant and often overlooked sections of the EMB such as the legal or operational divisions;
- externally, partner security agencies or CERT teams should be engaged to help resolve and de-escalate incident as appropriate, but also media, political parties, civil society and other actors that can increase the public trust.

EMBs are best served by taking advantage of all external resources and its full internal capacity to detect, monitor and respond to incidents beyond its (often limited) organizational capacity. CERT teams and other cyber security agencies should be involved in the planning, in order to clearly map roles and responsibilities, and finally during the incident itself, when a high level of cooperation is required. Simulations enable testing not only of internal capacities and preparedness, but also joint coordination and response mechanisms, in fact it is the only way outside of a real attack to identify vulnerabilities and hone crisis response strategies.

Getting Ready for the Next Election – The Ten Risks the CEC should mitigate

The following pages contain a list of ten electoral cyber risks relevant to the Ukrainian context. An effort was made to describe and address them in a general way so that the overview and associated recommendations could be useful to election practitioners in other countries as well.

IFES' HEAT risk assessment methodology is used to map vulnerabilities and threats, and to identify the 10 areas as the greatest risks with high impact on the election.

1. Cyber hygiene, establishing a culture of security awareness inside and outside the organization
2. Raising public trust and awareness, communication and institutional website
3. Resilience against malware, keeping everything updated, hardware & software
4. Human capacity building, challenges of retaining and training key personnel
5. Network monitoring and system activity logs, the importance of the cyber audit trail
6. The importance of cyber policy, standard operating procedures and IT code of conduct
7. Inter-institutional collaboration, creating an election crisis response team
8. Access to digital infrastructure, keeping an eye on all active devices
9. Access privileges and control, knowing who does what where at any time
10. Physical protection of digital infrastructure, protection beyond the digital realm

More information about the HEAT methodology is available in Appendix 2 of this playbook.

1. Cyber hygiene, establishing a culture of security awareness inside and outside the organization

Humans make mistakes. According to IBM's 2014 Cyber Security Intelligence Index[2], 95 percent of all security incidents involve human error. Cyber-hygiene is the means to protect and maintain IT systems and devices, and implement cyber security best practices. This is the most important tool organizations have to mitigate human error in cybersecurity.

Cyber-hygiene is the online analogue of personal hygiene, and encapsulates the daily routines, occasional checks and general behaviors required to maintain a user's online "health" (security).

The CEC has already started cyber-hygiene trainings, developed by IFES, the CEC is using a comprehensive and interactive cyber hygiene module, partly based on BRIDGE methodology, and specific to Ukraine. DECs will be also be enrolled in the course when they are formed.

The cyber hygiene training covers the following key good practices:

1. Detect and stop phishing/Spear phishing attempts
2. Password best practices
3. Data backup and protection
4. Updating software update and antiviruses
5. Clear desk and clear screen policy
6. Precaution when using USB devices
7. The dangers of the Internet of Things (IoT)
8. Social Networking

Other election stakeholders such as political parties or CSOs have different needs and could also be considering the following additional topics:

9. Administering social media pages
10. Use different channels for different types of communications
11. Use the cloud when it makes sense

There is fundamentally never too much cyber-hygiene training. All stakeholders, from political parties to media, CSO and all stakeholders involved in the election process should consider enrolling their staff into a training course before the election, and provide a refresher course before each electoral events.

[2] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

Recommendations for the CEC:

IDENTIFY & COLLECT:

- Regularly go through any existing functionality, operability and security plans, identify potential for human failure and include them into the cyber-hygiene curriculum.

EXPOSE:

- New staff should receive cyber-hygiene trainings when they begin employment, well before the beginning of the election preparation phase.

EXPLOIT:

- Finding the right balance between security and useability is difficult. The CEC, like all organizations, need to choose, and if possible, test cyber-hygiene recommendations on a small sample of users, and ensure high security impact with low user friction.

ADAPT:

- The IT/cybersecurity department should periodically review the most common threat vectors and evaluate associated risks and introduce cyber-hygiene measures to mitigate them. This includes the periodic changing of passwords and/or multi-factor authentication for email access, among other things.
- Cyber-hygiene training content should be updated regularly, and whenever possible, courses should be repeated before each election so that best practices have sufficient time to be understood and adopted (November 2019, and beyond).
- Combine cyber-hygiene trainings with a cybersecurity awareness campaigns that explains to how to communicate internally about cybersecurity risks.

Examples of exposures:

TECHNOLOGY: Many technology vulnerabilities are rooted in human exposure. The widespread use of pirated software could be a vector to deliver malevolent software to steal identities, spread malware and create backdoors into systems. Even if electoral mischief is not the original intent of the hacker behind malware distributed through pirated software, penetration of an electoral network could lead to a crime of opportunity when the hacker(s) recognize what they have infiltrated.

HUMAN: Busy humans become victims of convenience in many respects, particularly during the busy final preparation days of an election. Adopting habits that can limit exposure, such as being suspicious about any unsolicited email received even from close colleagues, takes discipline.

Executive assistants to managers or commission members, receptionists, inter-institution liaisons and employees of the communications department might be much more valuable targets to cyber predators than they may seem. Even experienced users may fall victim, typically by neglecting and underestimating new threats, as their previous knowledge becomes significantly and quickly outdated. For example, some power users, especially among IT staff, avoid installing antivirus software because of the performance overhead that such software may incur on a trusted workstation.

POLITICAL: Proper cyber hygiene is a common responsibility, shared at all level of the organization. All too frequently, IT departments inform the EMB management that patches have not been applied to servers, or servers might be using outdated and unsupported OS', but the EMB may decide that it is too costly, too time-consuming or too close to elections to engage in upgrades. The commission asks the IT department if the elections can be run without a major rehaul and expects the answer to be yes.

Attacks against auxiliary systems (systems that are not directly under the control of the EMB but that can have a significant impact on the election process) have been on the rise globally during the last 4 years, stressing the importance of cyber hygiene and cyber security in general, not only for the EMB but also for all election stakeholders. The most famous case is probably the hack of the personal email account (via phishing) of the chairman of a candidate campaign[3] during the U.S. presidential elections of 2016.

[3] https://en.wikipedia.org/wiki/Podesta_emails

2. Raising public trust and awareness, communication and institutional website

Transparency

Transparency is a key principle for credible elections and maintaining a high level of trust in the process is in the best interest of election authorities in general.

Cybersecurity measures aiming to protect elections are an additional challenge as it is difficult for EMBs to gauge which information can be made available to the public, to election participants or observers, to commission members and to IT security specialists in order to satisfy both the need for transparency and the need for confidentiality.

Website resilience

In addition to the challenge of transparency, EMBs have to ensure that their efforts to reach the public are not stopped by cyber attack on their public facing websites.

Websites are by design outside of the security perimeter, making them particularly vulnerable and more difficult to protect. They are also very often a challenge to keep uptodate, they are not replaced often enough and become very quickly outdated, obsolete and insecure. Modern, functional and easy-to-navigate websites that are content rich are what the electorate is already accustomed to in their everyday lives, they expect the same standard to be applied in terms of elections.

There is no way to prevent a DDoS attack from taking place — due to the open nature of the internet — but there are ways to dampen the associated risks, such as by creating multiple powerful mirrors which are transparent to the end-user, or by scrubbing traffic through a high-capacity cloud-based service.

Communication resilience

It is absolutely crucial that EMBs are able to keep open communication lines with the public, even when its website is under attack by DDoS or is defaced.

EMBs should have communication plans ready to quickly respond to most predictable incidents, these plans should be rehearsed and understood by all participants.

Recommendations for the CEC:

On transparency, and given previous issues faced during previous elections, the renewed CEC should seize the opportunity to clarify what information can or cannot be made public. In general, information should be considered not public if it can be misused by attackers if made available in the public domain.

As cybersecurity is a national defense issue, governmental security agencies may advise a more restrictive approach in information sharing due to threats stemming from disclosure of information to APTs.

IDENTIFY & COLLECT:

- Create and collect communication plans detailing crisis communication protocols and messages to be employed if there is an attack as it will likely occur during a busy election period where time to develop such protocols or messages is at a premium and may take away from other critical election communications.
- Establish a communication plan focusing on a successful attack on their results website, allowing the CEC to disclose maximum information possible without negatively influencing any investigation of the incident or further protection of the system.
- Review the needs of the CEC’s communications department. Increase their capacity

and necessary resources to communicate to election stakeholders about cybersecurity issues.

- Continuously maintain high standards with regards to the security of communication channels: the Content Management System (CMS) used by the current website should be up to date with the latest security patches, extra precaution should be taken to secure institutional social media pages before and during the election.

EXPOSE & EXPLOIT:

- Create a clearinghouse platform for information-sharing with cybersecurity and election stakeholders.
- Conduct pen tests on the CEC website, on the SVR (voter consultation) website and on the result publication website. If vulnerabilities are discovered, patch them and conduct new tests.
- Maintain the websites outside of the perimeter, and segregated. The CEC, the SVR and the result websites should not be consolidated on a single platform.
- When possible and politically acceptable, institutional websites should be hosted by specialized service providers who have dedicated security teams and high resilience against DDoS attacks. Under all circumstances, the CEC should prepare, maintain and regularly test plans for the mitigation of DDoS attacks against all websites, particularly during the critical period before elections.
- Simulate a situation in which the website is hacked and the EMB needs to respond to and recover from the incident. A communication strategy, as a part of comprehensive recovery plan should be clear and informative and details should be occluded only for the purpose of protecting the investigation or avoiding the danger of escalating the incident further. The communication department should be empowered to share information rather than seek permission to 'declassify' each item with the CEC management.

ADAPT:

- Reinforce the CEC website and increase the CEC's capacity for strategic communication. Ensure there is inter-departmental collaboration, especially between the Communications and IT departments.
- Evaluate the potential damage of keeping information from the public because of security considerations, consider that sophisticated attackers may have been studying the CEC's systems for months and will most likely not rely on publicly shared information for their reconnaissance.
- Inform the public about redundancy in data, systems that mitigate cyber attacks, and audit processes that detect and correct errors or alteration of data.
- Collaborate with media and NGOs on cybersecurity issues and build a network of supporters who will be able to communicate with the CEC and the public, in case of an incident compromising communication channels.
- Investigate a potential risk mitigation strategy by sharing election data early, at the local level. With election results, this can be materialized by having legitimate stakeholders (political parties, media, citizen observer groups, etc) collect election results (scans) at the local level. Their datasets can be compared with the officially published results to ensure there was no tampering with the CEC systems. This improves transparency and resilience of the election process.

Examples of exposures:

TECHNOLOGY: The EMB may decide to treat as classified most details of the system design, fearing that the disclosure of elements of the system architecture would benefit potential adversaries. Although this approach may have a strong appeal, it also introduces problems, because "security through obscurity" is generally not an effective security practice. It might prevent the EMB from seeking help from pen-testing or white hacker groups who might help find vulnerabilities that could be exploited by adversaries.

HUMAN: There are various tools to build websites. The technology choice should be carefully considered to favor security over simplicity and familiarity of the developer.

Communications staff need to be extremely careful in the way they handle devices. They should not have all accounts accessible from the same device (twitter, youtube, facebook and the website administration), because if this device is stolen and hacked the commission would lose in one hack all of its communication channels with the public.

POLITICAL: EMB IT departments are typically secretive about which cybersecurity measures to employ and which risks to accept, in order to prevent the leaking of vulnerabilities. In most situations, researchers, observers and other election stakeholders will not have the possibility to review any documentation that is in place. While an EMB might argue that it is not advisable to disclose any information about assumed risks outside the house, this should not extend to aspects of the functionality of election systems which are of legitimate concern to election stakeholders (such as results management or voter list systems).

The political risk of disclosing a successful attack of an election website might also justifiably make stakeholders question (or irresponsibly speculate about) the ability of the EMB to conduct an election free of manipulation.

LEGAL: If the election legislation and/or any legislation that governs the cybersecurity of critical infrastructure does not explicitly define which components and documentation should be made accessible and under what circumstances, the EMB might simply err on the side of caution and occlude from public view most information pertinent to cybersecurity.

Breaking into an election website rarely means that the election data is at risk of being altered, since data stored on an election website is generally a copy of main databases. However, in some cases, this intrusion may represent a breach of voter information privacy and may therefore be in violation of privacy protection laws, such as in the case of penetrating the website storing voter registration information.

PROCEDURAL: In an environment where cyberthreat can cause legitimate concerns to the legitimacy of an election, EMBs need to go beyond basic voter education campaigning (such as get-out-to-vote posters, online videos, etc.). EMBs who are not prepared to provide more detailed information for public consumption risk creating distrust. For example, in the event of a successful cyber-attack, an EMB who is trying to hide what happened, whether due to embarrassment or to some skewed perception that national interests are protected by not disclosing any details, may invoke fear, uncertainty and doubt about the election process.

3. Resilience against malware, keeping everything updated, hardware & software

Malware is an important tool for APTs when attacking a protected network. Adversaries will try to establish a payload (the component of a computer virus that executes a malicious activity) and hide it in the system. In industrial or business systems, APTs may have an interest in maintaining the presence of malware indefinitely for the purpose of prolonged espionage and illegal information gathering. However, if hackers manage to slip a destructive piece of software inside an EMB network, they are likely to activate it when it can do the most damage (to change election results online so they do not match the paper trail for example).

New and innovative malware designs are created all the time, as detection and protection mechanisms evolve in parallel. If facing a resourceful adversary, such as an APT, it is quite likely that adversaries are already aware of which antivirus software is in use in the organization; if the design of the malware is not very innovative, its detection is routine for any decent antivirus software.

The resilience of the EMB against APT will depend on its capacity to maintain an up-to-date and healthy environment for both hardware and software components.

Recommendations for the CEC

IDENTIFY & COLLECT:

- Periodically review the system architectures to identify outdated software or hardware components that need to be replaced or updated.
- Conduct a thorough penetration testing of both the RMS system, and potentially the SVR system before each election. Consider performing a compromise assessment in order to inspect historical logs for previously undiscovered intrusion.

EXPOSE:

- Scan periodically to see what devices are connected within the network and disconnect any unrecognized devices.
- Conduct a review to ensure that no unlicensed software is used on any computer in the organization

EXPLOIT:

- The IT department should stay ahead of the curve and constantly upgrade its professional knowledge. The period between elections is a great time for that. IFES is currently collaborating with the CEC of Ukraine to provide hardware- and software-independent advanced courses in cybersecurity.

ADAPT:

- Plan any substantial changes to the system, in terms of introduction of new hardware and software, well ahead of elections.
- Regularly ensure the segmentation of the network, so that the most sensitive networks cannot be accessible from the Internet. Air-gapping (physical separation) of the most sensitive equipment, such as voter list database server or results management server, is a must.

- Consider using hardened images to deploy to the computers connected to the critical network. Hardened images are specially configured versions of the operating system to focus on security.

Examples of exposures:

TECHNOLOGY: A failure to apply the latest security patches from the vendor of the hardware/software leads to technology exposure that can be exploited by adversaries. Although underlying issues might be of a human nature, they may also be due to organizational or policy issues that IT specialists could not tackle, such as unwillingness of the management to allocate resources to push for upgrades to the OS when needed. EMBs, which are typically struggling with insufficient resources or inflexible budgets, are especially prone to this problem.

Information flow, if not controlled, could be compromised: any point of access to the Internet, or more generally, access to everything outside the secured perimeter, is a potential exposure point for malware injection. From a cyber perspective, points of access that are not controlled or not visible by the EMB IT department are particularly vulnerable. The most common channels should be constantly monitored, including e-mail and web access as well as external media, such as USB flash drives.

HUMAN: Outdated and unpatched hardware and software lead to technology exposure. However, it is important that IT departments remain vigilant to newly disclosed vulnerabilities that can represent threats to the integrity of the system. New threats should be evaluated by EMB IT personnel to determine whether or not hardware is affected, and patch as needed.

POLITICAL: Even if IT personnel are aware of the threat spectrum, communicating this information to the management of the EMB can be a challenge. No matter their size, due to the critical nature of elections, EMB should assume that resourceful adversaries will have an interest in placing a carefully crafted malevolent piece of software within the EMB’s inner computer networks.

4. Human capacity building, challenges of retaining and training key personnel

While it takes significant time and money to procure hardware and set-up and configure the needed security applications, human capacity building is of utmost importance. EMBs typically have the same salary rates as government institutions, which are far from competitive with the private sector. Retaining highly qualified personnel is a big challenge in many countries and Ukraine is no exception. IT specialists need to understand how systems used for the protection of the infrastructure work in order to defend them against APTs. Additionally, EMBs do not usually have the capacity to act alone, and depend on external contractors or CERTs in many countries.

Recommendations for the CEC:

ADAPT:

- Obtain waiver from the civil service administration to be able to pay cybersecurity experts and IT personnel above the public service pay scale.
- Incentivize employee retention through long term training programs.
- Employ interns and young professionals and offer long term career opportunities to delay the turnover.
- Review existing employment practices in order to maximize recruitment of the most qualified personnel: cybersecurity specialists in the EMB should have a specialization and/or equivalent experience in IT security.

Examples of exposures:

HUMAN: Some EMBs may face serious problems retaining qualified IT specialists and experience a high turnover. This problem is exacerbated by the fact that most EMBs do not have dedicated cybersecurity experts, but must rely on non-specialized IT specialists.

POLITICAL: The problem of potentially inadequate compensation for the work of EMB IT specialists is typically connected with the salaries of IT workers in the public service in general, since usually EMBs fall into that bracket. Therefore, addressing this problem could mean addressing pay scales for the IT and cybersecurity workers in the public sector or petitioning for an exemption within the EMB to pay cybersecurity IT specialists at more competitive rates.

5. Network monitoring and system activity logs, the importance of the cyber audit trail

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

The cyber audit trail is an indispensable tool for the defense of the integrity of a network and of the election as a whole.

For example, it can help you reconstruct events, detect intrusions, and analyze problems such as poor performance or unexpected system behavior. It can also help promote good behavior and a sense of accountability among users, if they know that their actions can be reviewed.

The issue of monitoring of the system and networks is not only a technical one. The IT department should set up all the components to log events and traffic, but also have resources that can analyze the mountain of newly created log data.

Recommendations to the CEC:

IDENTIFY & COLLECT:

- Ensure that the process of monitoring all system and network events for SIEM are in place. Periodically review the procedures, policies and configurations in place to ensure that they record all information necessary to a holistic cyber security analysis.

ADAPT:

- Have protocols in place informing how to react based on types of critical event detected in the system. The necessary actions to respond to or recover from the problem are as important as detecting it.
- Ensure that the data capture and analysis is tested before the election period. This will allow the administrators to see normal pattern and distinguish potential anomaly on time.
- The SIEM should be used holistically if possible recording network events on the SVR network, the RMS network, and in in the CEC internal network.
- Insider attacks can be indirectly but efficiently addressed by implementing efficient network monitoring and analysis of log files.

Examples of exposure:

TECHNOLOGY: No matter how many protections have been established around the critical network and server infrastructure, EMBs need to be able to to detect and react in case of incident, whether a cybersecurity intrusion or a hardware malfunction. Without a cyber audit trail, the EMB cannot to establish the origin and location of the problem.

HUMAN: EMBs must fully understand that cybersecurity risk mitigation and vulnerability management require different skills from knowing how to set up a network for results data entry or design a voter list database. The IT department of an EMB should either have personnel who possess, among other skills, advanced knowledge of cybersecurity, or employ dedicated personnel for that purpose. If the EMB is not familiar with sophisticated mechanisms to monitor its systems, this reduces its resilience against cyber attacks significantly.

LEGAL & PROCEDURAL: The cyber audit trail must be safe from alteration to prevent illegal activities and ensure appropriate checks and balances. The cyber audit trail is essential to the EMB to prove what is happening and what is not happening inside its security perimeter, and hence to make sure no critical election process has been affected. It can and has been used in court of law in election related cases to prove intrusion in the network.

6. The importance of policies, standard operating procedures, and a code of conduct

Cybersecurity policy should inform operators of their responsibilities to protect the technology and information assets of the EMB. It should describe the controls and the best practices to be followed by the operators while conducting electoral operations.

Companies, particularly in highly regulated environments such as the financial sector, have long adopted policies and strict operating procedures for their staff. Many EMBs have strict procedures for counting for example, but often lack the same level of details when it comes to data management and proper use of technology. This is a weakness that EMBs cannot afford any longer.

Software development is an important aspect of standard operating procedure which cannot be understated. It can materialize with the implementation of strict supply chain controls and procurement rules, or with protocols to verify the origin of the source code during the deployment of a new version of the software.

Recommendations for the CEC:

IDENTIFY & COLLECT:

- Introduce a cybersecurity strategy and risk mitigation framework based on the legislation of the state or internationally recognized cybersecurity standards such as the cybersecurity framework by the National Institute of Standards and Technology (NIST) of the ISO 27K family.
- Introduce formalized threat modeling and risk management in relation to system design and implementation, detailing all security assumptions, as well as action plans for response and recovery.
- Develop and ask staff to sign a code of conduct defining acceptable use of professional and social media platforms. CEC and DEC staff should restrain from social media activities during working hours in the election period. Staff should not “check-in” or share their locations or travel itineraries.

EXPLOIT:

- Periodically review and compare snapshots of data, review the number and type of changes in the SVR to ensure integrity of data. Accompany the snapshots with transaction reports showing all updates to the register, providing a complete audit of changes.
- Conduct internal and external source code audits, after any changes (especially significant changes) to the SVR system have been implemented.
- Make source code versioning available, and all changes traceable to the author and date of modification.
- Restrict all access to database from systems accessible from the internet to executing carefully designed stored procedures (SP) using the minimum required security authorization.

ADAPT:

- Consider conducting a systematic check of all cybersecurity procedures through internal and, potentially external, audit procedures (to avoid conflicts of interest when implementing and auditing).
- Review SVR backup and emergency recovery plans. Implement redundant systems, even on scaled-down hardware, to allow failover in case of an attack on or failure of the primary system.
- Establish and test system and data recovery in the event of data loss should be established as a policy and an institutional commitment.

Examples of exposures:

HUMAN: Clear procedures and policies ensure EMB staff know what is expected of them. For example, the IT department should have clear direction that no code should be deployed that has not been properly tested.

Without clear code of conduct, a staff visit to a conference could be used as a reconnaissance tool to create a spearphishing email. Any check-in to a location related to the EMBs work with the election could trigger targeted attacks on the facility from an attacker who aims to disrupt operations.

7. Inter-institutional collaboration, creating an election crisis response team

Collaboration among institutions is often an important measure to increase the preparedness of cyber protection. While this is a very natural measure to introduce among government agencies, EMBs need to safeguard their independence from governments. Cybersecurity is one of the fields in which such collaboration is needed as national security may be at stake, and EMBs are poorly equipped to address highly sophisticated threats.

EMBs should also collaborate with other election stakeholders, such political parties on a regular basis to create a common understanding of the essential issues related to integrity of the electoral process and will help to avoid unnecessary speculations that usually arise due to lack of information.

Increasing cooperation with CSOs and media is another step that EMBs typically need to take to increase the transparency of elections, and election CSOs in many countries are taking a heightened interest in cybersecurity.

Recommendations to the CEC:

IDENTIFY & COLLECT:

- Ensure that collaboration with government institutions, including SSSCIP and the SBU are formalized, public and transparent, in order to maintain trust in the independence of the CEC. The mandate of each member of the election CERT team should be clearly understood by all parties.

EXPOSE & EXPLOIT:

- Inter-institutional collaboration should be carefully planned in the wider context of the Business Continuity Plan, if such plan exists, or the equivalent cybersecurity plan. Based on this plan, the inter-institutional working group should be able to react swiftly and take appropriate action suitable to answer the cybersecurity incident.

ADAPT:

- Request periodic review of the level of protection in place on the underlying systems and any associated risks for the relevant institutions, given the dependence on external networks for transfer of election information, including voter register data.
- Work with the SSSCIP to allocate sufficient resources to conduct diligent pen tests, given the nature of the APT threat. Request that test are performed early enough to provide the possibility to mitigate newly discovered vulnerabilities and, if needed, conduct additional tests.

Example of exposures:

TECHNOLOGY: Collaboration and communication are as necessary as system and network monitoring sensors, when an EMB teams up with a CERT team. A lack of collaboration at the working level through well-established information sharing may lead to inefficiency and undetected threats.

HUMAN & POLITICAL: If the collaboration efforts put in place serve only bureaucratic purposes and are not of real value, the EMB will not benefit at all. On the contrary, such limited or soft collaboration may block the EMB from seeking substantial assistance from other source, and result in them assuming responsibility for unaddressed vulnerabilities.

LEGAL: Both the real and perceived independence of EMBs from government interference may have a significant impact on the confidence of the electorate that the elections are conducted on a level playing field. If the nature of the collaboration with government institutions is not well-founded and transparent this may hamper the ability of the EMB to administer elections as an independent election commission. The situation should be avoided in which inter-institutional collaboration leads to a real or perceived conflict of interest in which the EMB Secretariat is perceived as an extension of the government, rather than answerable to the independent EMB.

PROCEDURAL: Even though a working collaboration with the government may already be in place, in some cases there are no procedures on how this collaboration would be implemented, especially if it needs to respond to a cybersecurity incident. There is a risk of improvisation or hasty decisions during an already busy election administration period.

8. Access to digital infrastructure

Equipment left unattended or poorly secured are opportunities for adversaries.

Good practice is to ensure that all computers are locked for use after a relatively short period of inactivity and to ensure that someone is personally responsible for each and every critical component in the inventory.

Recommendations for the CEC:

IDENTIFY & COLLECT:

- Access to the most sensitive equipment, such as the server containing the voter register database, should be logged redundantly, i.e., both electronically and on paper. Access to external ports of servers and workstations used for access to critical systems should not be allowed and should be strictly adhered to.
- Enforce strict right to access. For example, revoke access to former employees immediately after they leave their jobs.
- Ensure, through the review of system designs and periodic checks, that all critical components and internal networks of election systems are segmented or segregated (air-gapped) from the rest of the networks and the Internet. Computers used for handling emails and general-purpose browsing should not be wired in any way to the networks holding sensitive elections data.

EXPOSE & EXPLOIT:

- Familiarize management with access procedures. They should review and endorse such procedures. The CEC could consider formalizing these procedures and decide whether to maintain them as an internal document only, depending on the level of details described in the documentation outlining such procedures.

ADAPT:

- Do not allow full access to servers and configuration of other devices by only one person, always do so in pairs to ensure security cross-checks.
- Install video surveillance to entry/exit points where sensitive hardware is located, avoiding pointing cameras at terminals connected to servers to avoid filming login credentials.
- Take a restrictive approach to access: physical access to sensitive hardware should be agreed upon and/or allowed only in special monitored circumstances, preparing for for the possibility of unfettered access to registered observers and auditors during the election period so that they can be reassured that the security measures are implemented.
- Ensure that wireless connectivity is switched off on the election critical system that does not require it. All physical ports and terminals connected to servers should be sealed and physical connection to any devices needs to be performed for a very good reason and to be documented.

Example of exposures:

TECHNOLOGY: Sensitive devices can be compromised, even by IT specialists who are considered trusted employees. The threat can be associated with the way the servers are accessed and the dynamics of accessing the servers in a specially protected environment. The threat can also be associated with a much simpler but potentially fatal threat of leaving an unlocked laptop unattended. Critical networks should never, for example, be accessible over wireless connections. Tamper-evident sealing tapes should also be put on USB and other ports on critical devices to prevent deliberate or accidental introduction of malware in the system.

HUMAN: A visit to the server room should be viewed as a potential security breach. The danger of an insider attack in Ukraine is significant and can come in the form of unauthorized access to workstations, private computers, routers and data servers. In case of insider attack, the delivery of malware through unrecorded access to a colleague’s unattended workstation is a possible attack vector that does not require special IT skills by the insider.

POLITICAL: An over-reliance on external institutions that do not bear direct responsibility related to the election process, such as vendors, subcontractors or even government institutions, can lead to additional human exposure and potential security breaches.

PROCEDURAL: In the absence of prescribed access guidelines, the potential of a relaxed access policy, for example between elections when there is less alertness about security, can lead to additional human and technology exposure.

9. Elevated access privileges and inadequate controls

Physical access is usually not sufficient to tamper with a computer through a terminal. However, as long as a connection is maintained, most computers can be tampered with remotely. A good cybersecurity assumption is that if the computer is not physically disconnected from a network, it can in theory be accessed remotely, regardless of any claims to the contrary.

Large organizations have generally adopted the approach to carefully consider Identity and Access Management (IAM) policies. For example, an EMB chairperson may request the IT administrator give her administrative access to her laptop so that she can freely and confidentially install the software she wants. This may be convenient for the chairperson but is definitely not advisable in terms of good cybersecurity practice. The IT administrator (who in a smaller EMB may be doubling as a cybersecurity officer) would find it difficult to refuse the chairperson, and could be henceforward unaware of what software is installed on the laptop.

It is important that all users follow established rules. The security of any system is as strong as the weakest link, and this is also true of cybersecurity of election systems.

Recommendations to the CEC:

IDENTIFY & COLLECT:

- Conduct periodic reviews of access policies for all employees. Consider the access policies of election stakeholders to election data: it should be known if the users, especially employees, understand what is located where in the system and what is an acceptable use of information and what is not.
- Review the policies for backend access to live election data for both the SVR and the RMS, to ensure that incorrect updates and unauthorized changes are not introduced accidentally or deliberately.

EXPOSE & EXPLOIT:

- Test that policies are implemented. For example, check occasionally whether all retired accounts are deactivated, or whether adjustments in the interconnectivity of components require review of whitelisting (or blacklisting).
- Clearly allocate of responsibility, and define a work plan that outlines security procedures, such as with regards to the access to servers. This will be critical to mitigate the danger of an insider attack.

ADAPT:

- Maintain segregation of duties between system administrators who configure the operating system and install required software, and security administrators who review changes in configuration files and logs, and will not have permission to access or handle any sensitive (election) data. In any case, the number of IT specialists with administrative access to core components of the system should be strictly limited.
- Consider appointing an Access Security Auditor, ad-hoc or permanent, to conduct periodic inspections, identify weaknesses and ensure enforcement of policies in relation to access control.
- Consider vetting of staff when/if possible

Examples of exposures:

TECHNOLOGY: The choice of the operating system (OS) may dictate certain aspects of how the privileges are assigned. All modern operating systems have sophisticated tools for user rights management, but the administrators must be well-trained about the possible consequences of various configurations in order to provide functional access as required while preventing privileges which the users do not need. For example, there is no good reason for a single CEC member to have superuser access to a voter register database. On the other hand, there are some bad reasons why a CEC member would have such access, such as to take a snapshot of the voter registration database and share it outside of the controlled environment for political gains.

HUMAN: The lack of training of administrators in both OS-dependent and OS-independent aspects of user rights management could significantly increase technology exposure. The organization's management may be too lax and allow the degradation of policies for administrative privileges simply for the convenience of users.

Allocation of user accounts that are not personalized can reduce the accountability of individual users of election systems and should generally be avoided. In other words, it should be possible to trace all logged access back to a user.

POLITICAL & LEGAL: Strict policies on access could lead to reduced transparency of elections, if not carefully balanced. For example, administrators should investigate which actions can be performed within a system without the need to identify users. Lack of access of election stakeholders such as political parties and civil society to data that is not sensitive can reduce the accountability and transparency of the EMB. At the same time, public and access restricted systems should be isolated to exclude the possibility of accidental access to classified information by a non-authorized user.

PROCEDURAL: Having no procedures for access rights can lead to confusion and a variable institutional approach. A lack of a comprehensive documentation detailing access privileges can lead to hidden issues. All personnel should be informed about the procedures in writing and confirm the understanding of the policies.

10. Physical protection of digital infrastructure

Ukraine is facing an adversary that is engaging in hybrid warfare and is not shying away from any means of aggression. Physical attacks on infrastructure may be used to sow fear, disorder and confusion, but can also be used to destroy IT infrastructure.

Recommendations for the CEC:

IDENTIFY & COLLECT:

- Conduct coordination and/or working group meetings with the state/local agencies legally mandated to provide physical security. Assess if sufficient emphasis is placed on protecting digital assets.
- Go through the planning of physical security perimeters and clarify guard shifts and plans for increased security during elections.
- Study the history of previous security incidents, identify details of the incidents: the goals, victims and perpetrators, damage.
- List critical equipment and materials, identify potential vendors and service providers who can immediately provide support in case of emergency.
- Assess and map the potential damage to the election processes in case of physical sabotage, using the election calendar, workflow and schemas of security perimeters.

EXPOSE & EXPLOIT:

- Establish which physical security risks are accepted and re-assess the need to mitigate them.
- Find key points of vulnerability and list them. Test if any points of security are not properly planned.
- Conduct simulations of election day activities and contingency plans.

ADAPT:

- Create a thorough security plan or review the existing plans using lessons-learned in the planning phases.
- Plan a detailed set of contingency measures of resuming election operations in case of an incident.
- Conduct and repeat security simulations with updated plans periodically and before each election.

Examples of exposures:

PROCEDURAL: Well-planned and coordinated attacks can be designed to target servers, telecommunication nodes and other critical equipment. During critical periods of an election, such as approaching legal deadlines and election day itself, physical attacks can be a very effective disruptive tool. For example, an adversary may attempt to disrupt the tabulation of election results in a sufficient number of districts in order to delay the publication of results or to sow doubt in the electoral outcome.

Appendix 1 – Timeline of the most significant hacking attacks on Critical Infrastructure in Ukraine

May 2014 – Attack on the CEC

Just three days before the early presidential election, a hacker group activated a previously installed malware at 3 a.m. and wiped clean components of the RMS and all online backups. It took the CEC almost three days to relaunch the system with the use of offline backups, which were ready only one hour before the opening of the polls.

It is not clear how exactly the malware was planted. The pro-Russian group Cyberberkut claimed responsibility, but it is suspected that APT28 was behind the attack which was followed by a DDOS attack and a failed attempt to plant fake results on the CEC website.

October 2015 – Attacks on media outlets (BlackEnergy)

Although the BlackEnergy trojan is known to exist since 2007, advanced variants (BlackEnergy 2 and 3) were detected in Ukraine in mid-2015 as a macro in Microsoft Excel and Word documents. There are indications that it was already present in Ukraine in 2014.

In late 2015, antivirus company ESET discovered that the BlackEnergy trojan was used as a backdoor to deliver a very destructive KillDisk program in an attack against some Ukrainian media outlets during the October 2015 local elections. This use of KillDisk in Ukraine was first documented by CERT-UA. The attack attempted to destroy specific types of files in media organizations (such as all audiovisual files) in order to do maximum damage to media outlets.

December 2015 – Attacks on power distribution companies (BlackEnergy)

The energy sector in Ukraine was a major target for APTs in 2015. The BlackEnergy attack of December 2015 is the first successful cyber-attack on a power grid in history. The attack led to blackouts for several hours in three different regions in Ukraine and affected approximately 300,000 citizens. It is believed that APT Sandworm (APT28) was behind these attacks.

The trojan was delivered to the computer networks of power distribution companies through phishing emails and managed to install malware to provide backdoors and remote access to these networks. The hackers managed to get control over the SCADA management workstations to switch off power distribution and subsequently wiped data from workstations in order to prevent tracing of the intrusion.

January 2016 – Attack on the Boryspil Airport (BlackEnergy)

Another incident during this period related to critical infrastructure was the discovery of BlackEnergy malware samples on Boryspil Airport workstations. Although no attack occurred, the potential for serious damage prompted Ukrainian authorities to enhance the cybersecurity of critical infrastructure.

December 2016 – Ministry of Finance and State Treasury

An APT, using an unknown means of delivering a payload, managed to infiltrate the Ministry of Finance and the State Treasury and destroyed main databases from their servers using KillDisk.

The attackers’ goal was to completely disrupt the state financial system at the end of the year when most budget payments are made. The attackers managed to prevent payments of a high number of transactions, reportedly worth hundreds of millions in Ukrainian Hryvnia.

December 2016 – Attack on Kyivenergo (Industroyer)

During this second successful attack on power grids in Ukraine, parts of Kyiv were left in the dark for one hour. The novelty of the attack was that the malware used was developed for industrial control systems that do not operate ordinary computer networks (IP communication protocol) for information exchange.

The identified malware was dubbed Industroyer, or Crashoverride. It is a modular malware comprising a backdoor, program launcher, four different payload components and a data wiping utility.

December 2016 – Attack on Ukrzaliznytsya IT systems

A significant cybersecurity incident achieved control of the systems of the largest Ukrainian company, Ukrzaliznytsya. Although the available information is limited, it was reported that hackers used malware and remote access to the company network to bring down the company’s website and some transportation management systems, which resulted in serious delays in train timetables.

June 2017 – Attack on Ukrainian companies ((Not)Petya)

The (Not)Petya attack is considered to be the biggest global cybersecurity incident until to date. The malware was delivered to a huge number of companies through an update of the popular financial software package M.E.Doc.

The attack, later attributed to APT Sandworm (aka APT28), first managed to hack into M.E.Doc headquarters and create a backdoor to the financial software’s update server, which at the time used an outdated and unpatched OS.

The malware encrypted the contents of the hard disk of infected computers and requested payment of 300 USD through cryptocurrency. However, the malware only masqueraded as ransomware as no decryption keys were sent to users who paid.

The extensive damage of (Not)Petya was not limited to Ukraine, as it also affected a significant number of international companies.

October 2017 – Attack on Kyiv Metro and Odesa airport (BadRabbit)

A smaller-scale but still significant ransomware attack affected transportation companies, including Odesa International Airport and the Kyiv Metro. As with (Not)Petya, BadRabbit encrypts hard disk information for blackmailing. It is unknown (or undisclosed) who perpetrated this attack in Ukraine.

Appendix 2 – The Holistic Exposure and Adaptation Testing (HEAT) Process

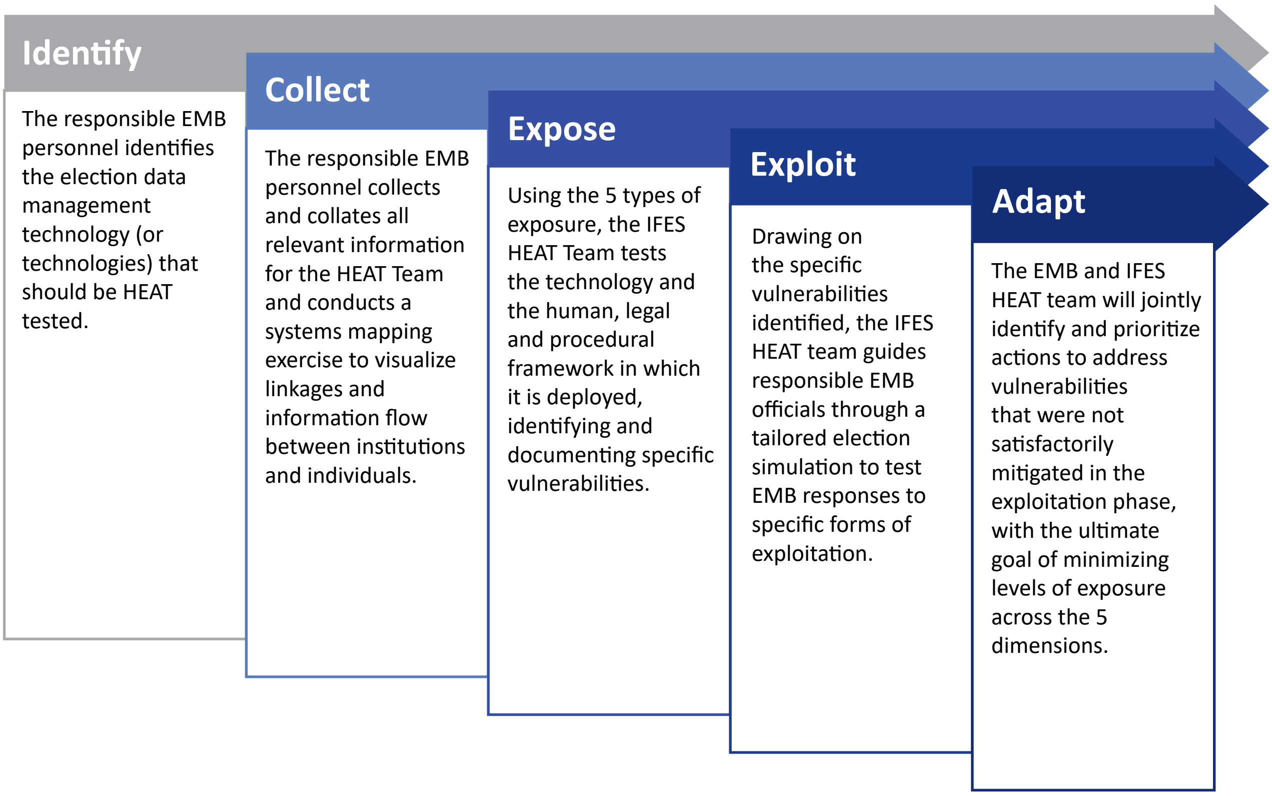
IFES' HEAT Process is a process for simultaneously identifying and testing the potential exploitation of vulnerabilities in the use of election data management technology. HEAT tests the technology itself, as well as the *legal and operational frameworks* in which the technology is being deployed. In contrast to a technology certification or basic testing process, the HEAT Process is a holistic way to examine vulnerabilities and ensure they can be corrected, communicated, or managed. For example, in a traditional certification process, a certain technology platform may be tested to ensure that data is secure. The certification process would not, however, prepare the EMB for a simple website disruption that could severely damage the institution's credibility with the public, regardless of whether the data remains free of errors or incursions.

Drawing on themes, trends, and approaches from the literature, IFES has identified five different types of exposure an EMB must consider in its use of data management technology platforms – technology, human, political, legal, and procedural. These different types or "dimensions" of exposure have in turn informed the development of the HEAT Process. IFES aims to incorporate elements of existing testing processes within a straightforward, holistic testing process that can help an EMB correct vulnerabilities in these five areas that could lead to manipulation of election data (known or unknown), system failure, or future legal challenges. The HEAT process is not a mechanism to approve or to reject the decision to use a particular technology or a particular vendor, although it can inform effective vendor relationships and a strategy for cyber-technology supply chain threats, as well as the interaction between different technology platforms that might be used in different parts of the electoral process. A HEAT process can also help an EMB prepare for the resources and processes they will need to have in place if a security breach or system failure occurs, or if the system is challenged in court. This is particularly important with respect to the type of evidence required and admissible with respect to election technology, and to establish a chain of evidence that can be used in future legal challenges. ICT officials need to work closely with legal officials within an EMB to address this vulnerability.

As with all aspects of the electoral process, positive public perceptions and public trust are critical to the credibility of elections and the acceptance of results. The HEAT process is designed to help reinforce with political stakeholders and the public the risk-mitigation measures inherently needed for the proper use of election technology, and the importance of contingency planning. Ultimately the HEAT process aims to increase public confidence in the electoral process, and to help EMBs to exercise (and document) due diligence measures. However, because the HEAT process focuses on identifying vulnerabilities, it must be carefully managed and communicated to build, rather than erode, public confidence in the EMB and in the technology. Hence, an EMB must ensure it has enough time and resources to address the issues that are found, or these vulnerabilities could be exploited to call into question various aspects of the process, from the validity of the voter register, through to the legitimacy of the election result.

The HEAT process is composed of five steps, described in more detail in the next section: Identify (the EMB identifies the technology to be tested); Collect (IFES works in collaboration with the EMB to collect relevant information, including a systems mapping exercise); Expose (using the framework of five exposures described above, IFES works to identify vulnerabilities in the technology for each exposure); Exploit (IFES conducts a simulation exercise with the EMB, based on the vulnerabilities discovered in the previous two steps); and Adapt (the EMB and IFES jointly identify the priority actions necessary to protect the electoral technology against these vulnerabilities).

Outlining the Holistic Exposure and Adaptation Testing Process



Identify

The responsible EMB personnel identifies the election data management technology (or technologies) that should be HEAT tested.

Collect

The responsible EMB personnel collects and collates all relevant information for the HEAT Team and conducts a systems mapping exercise to visualize linkages and information flow between institutions and individuals.

Expose

Using the 5 types of exposure, the IFES HEAT Team tests the technology and the human, legal and procedural framework in which it is deployed, identifying and documenting specific vulnerabilities.

Exploit

Drawing on the specific vulnerabilities identified, the IFES HEAT team guides responsible EMB officials through a tailored election simulation to test EMB responses to specific forms of exploitation.

Adapt

The EMB and IFES HEAT team will jointly identify and prioritize actions to address vulnerabilities that were not satisfactorily mitigated in the exploitation phase, with the ultimate goal of minimizing levels of exposure across the 5 dimensions.

Identify

The HEAT process is designed to be EMB-led, and to provide a capacity-building element for the EMB, as opposed to an external assessment. As such, the first step of the HEAT process is undertaken by the EMB itself, with technical assistance as needed, and requires the EMB to identify which election data management technology (or technologies) should be HEAT tested. The HEAT process focuses primarily on electronic systems or platforms related to election processes that include any forms of automation or are digitalized, such as voter registration, voter identification, voting and vote count, and results transmission and tabulation. Depending on how advanced the management system is, it can also include candidate registration, the ballot design (in complex elections such as local elections), and ballot printing. One or more of these can be tested, as relevant and applicable to the country in question, and the HEAT process is designed to target these systems and processes. However, depending on the EMB's mandate and specific circumstances of the country in question, there may be other relevant data management systems or platforms that an EMB may wish to test, such as political party registration databases, campaign finance databases and reports, systems for redistricting of constituencies and precincts and polling station allocation, procurement/inventory databases, personnel and financial databases, website and social media platforms, and case management systems used in complaints adjudication.

Apart from identification of assets that need protection, the EMBs should be in position to evaluate the likelihood of any looming cybersecurity threats, be it DDOS attacks or insider attacks, spear-phishing or an exploit through malware. Listing all possible threats and including an assessment of how imminent the danger is helps to prepare for the further steps in the HEAT process.

Collect

After identifying the specific election data management technology to be HEAT tested, the relevant EMB staff should collect and collate all relevant information for the HEAT Team. This includes laws, rules, procedures, manuals, and training material, formalized strategic policies – if any – on the one hand and the technical information such as system design (schematics), data security policies, set-up and configuration scripts, program source code, and other relevant material, on the other. It will be important to collect all relevant laws and rules so the HEAT team can identify provisions in the legal framework that may be used to challenge election technology and data management processes later in the election process, to ensure adequate regulations and policies are in place to govern the use of the data management technology, to ensure roles and responsibilities are clarified (especially between EMBs and technology vendors) and to identify contingency measures. The relevant laws and rules will include the constitution, national electoral laws, EMB regulations, any other relevant national laws or rules on data management, data protection, or cybersecurity, laws and rules on civil procedure and evidence, and relevant national case law, where applicable. In addition to these legal materials, the EMB should collect all relevant policies, procedures, strategies, operational plans, guidance documents, manuals and training materials used in the electoral process that are relevant in whole or in part to the election technology being tested.

During the collection phase, the EMB will also conduct a system mapping exercise to visualize components of the system being HEAT tested, as well as linkages and information flow between institutions and individuals. System mapping is a tool within the larger research method of systems thinking that visualizes linkages among key actors. Often individual and institutional connections, or lack thereof, can impact the election process. The links that the EMB holds with any other authority within the country, other independent agencies or government agencies dealing with data protection should be clearly identified at this stage. The cybersecurity community is unified in saying that sharing of cybersecurity information is critical for adequate protection and resilience and the election process is not an exception to this. What is exceptional about the elections, however, is that the independence of the EMB must be maintained, regardless of any collaborative efforts. The IFES HEAT team will provide instructions and templates for the mapping, or can directly guide the EMB through this process. The resulting map will form part of the HEAT team's exposure process in step three.

Expose

Step three requires the HEAT team to collectively analyze the relevant EMB materials and systems map and expose vulnerabilities within the five different types of exposure – technological, human, political, legal and procedural. Because the process looks holistically at these five different types of exposure, the HEAT team should generally consist of a technology expert, legal expert, and election operations expert. Step one of the HEAT process should feed into the identification of the HEAT team, in terms of the specific technology or technologies being tested. The core question will be: who is qualified to help test and assess the election technology and the framework / context in which it is deployed? Once identified, during this part of the process the HEAT team will identify and record vulnerabilities that the EMB faces in using the specific technology being tested, categorized under the five types of exposure, and will list preliminary options for mitigating or managing vulnerabilities.[4]
In addition, the HEAT team should look at certain external elements that can significantly impact on the election process, especially in terms of possible negative influence or disinformation campaigns against the EMB or other election stakeholders, and will examine existing EMB communication strategies.

[4] Over time, IFES will develop a global database of vulnerabilities and recommendations as the HEAT process is utilized with local partners. This can serve as a reference tool for EMBs and technical assistance providers.

Exploit

Drawing on the specific vulnerabilities identified during steps two and three, the HEAT team will guide responsible EMB officials through a tailored election simulation tabletop exercise (TTX) to test EMB responses to specific forms of exploitation. A TTX is a training simulation that mirrors real world conditions, uses an accelerated timeline to increase pressure, gives everyone a role with corresponding responsibilities, and enables participants to absorb information, make decisions, and execute plans. It is similar to the "red-teaming" process used by the U.S. Department of Defense to "challenge emerging operational concepts in order to discover weaknesses before real adversaries do."[5] The HEAT team will draw on the vulnerabilities identified in step three of the HEAT process and test participant responses as these vulnerabilities emerge or are exploited in a simulated environment. This step has two purposes – testing existing capacity and responses of EMB officials, and serving as a more impactful learning exercise for officials who will be responsible for making necessary changes to reduce EMB cybersecurity exposure. Lower-level commissions require substantial training related to the election process, in general, and cybersecurity is no exception.

Cybersecurity is a set of measures put in place and actions taken to identify exposure to threats to digital networks and safeguarded information; to protect digital information (and related physical) assets from stealing, exposing, destroying or altering; to detect that an incident has occurred inside a system domain; to respond to an attack; to quickly recover from a successful breach.

The TTX can help reveal and emphasize for EMB officials the exact training needs required for different staff in the EMB, for example around cyber-hygiene and spear-phishing. It will be adapted to the vulnerabilities discovered in the HEAT process and to the broader electoral context in which the EMB's technology will be used. The TTX will end with a debriefing to discuss lessons learned and to identify responses to remaining vulnerabilities, which will provide the basis for the action plan the EMB and IFES will define in the next and final step.

Adapt

The final step of the HEAT process is a collaborative de-briefing exercise and strategy session with the relevant EMB officials. This session will aim to identify and prioritize actions to address vulnerabilities that were not satisfactorily mitigated in the exploitation phase, with the ultimate goal of minimizing levels of exposure across the five dimensions. The session will consider who has responsibility to fix or correct vulnerabilities, short and longer-term cost considerations, time considerations, and transparency and communication.

In terms of technology exposure, some of the essential tools that EMBs might consider using to avoid system crashes are carefully designing systems, testing, set-up, configuration, piloting, audits, and contingency planning. EMBs should have back-up plans for new systems, including the possibility to revert to old systems in the event of a crisis. For example, if seat allocation is relatively complex, the commission that bears responsibility may decide not to rely exclusively on software being used for the first time, even if that software has been tested.[6] EMBs should have advanced network-monitoring capabilities to determine with some level of certainty the nature of events that occur in its systems. Having a strategy in place would allow EMBs to react quickly, to apply contingency plans, or to restore from backups.

[5] Defense Science Board Task Force, The Role and Status of DoD Red Teaming Activities, United States Department of Defense, September 2003, https://fas.org/irp/agency/dod/dsb/redteam.pdf.

[6] In Denmark during the 2009 European Parliament elections, Statistics Denmark used seat allocation software but also informally had MS Excel spread sheets as a backup to check that their calculations were correct.

In terms of human exposure, measures against insider attacks are often self-explanatory – such as monitoring physical access to servers – but sometimes additional action may be required. This can entail doubling up IT experts when logging in to sensitive servers and never using wireless networks for sensitive LANs to avoid close proximity fraudulent Wi-Fi access attacks (so-called evil twin attacks). Control systems must be in place to ensure accessibility is strictly compartmentalized, logs created, and logs regularly reviewed by ICT-supervisors for compliance and abuse. Vetting personnel when hiring is good practice, but needs to be conducted carefully to avoid nepotism or discrimination and to avoid introducing new problems, such as potential bureaucratic delays. A good EMB should also have a data security strategy to avoid having outdated, obsolete, or underutilized election systems that can lead to inefficient data management.

For political exposure, EMBs should carefully plan and execute procurement processes for election technology, and should develop sound communication and consultation mechanisms on cybersecurity issues. Specific measures may also need to be put in place to strengthen the de jure or de facto independence of the EMB and its leadership. At the same time, greater collaboration may be required with law enforcement personnel and intelligence agencies, depending on the nature of the cyber threat. This would need to be done carefully, recognizing the need for the EMB to also maintain independence both in practice and in terms of public perceptions. For legal and procedural exposure, various legal or regulatory amendments or reforms may be required, along with the development or refinement of strategy documents, operational plans, training materials, or other manuals and guidelines.

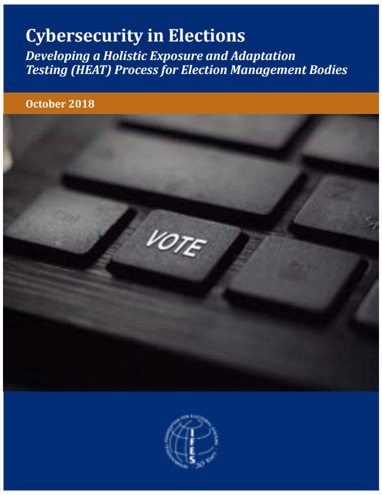
The EMB may have certain cybersecurity practices in place, but those might be scattered in multiple documents, informal files kept by the IT specialists, or not even committed to written form, but only employed in practice. The HEAT Team should encourage the EMB to consolidate and lay down all their security practices and assumptions in one place. In doing so, those practices and assumptions will be made more accessible and transparent to the EMB, and will be made mutable (for example, if the system does not place any constraints on the size and structure of passwords, this can be highly problematic). This, if formalized, can become the EMB's cybersecurity strategy. The establishment of such a strategy will increase the EMBs resilience against cyber attacks.

The specific recommendations and actions born of this final step will depend on the information from the previous steps. Examples of actions identified in the 'Adapt' step are cyber hygiene courses for EMB employees, a cybersecurity playbook designed for the EMB, and assistance in procuring new technology. Ultimately, the goals of the HEAT process are to holistically test specific election technology systems for vulnerabilities, to directly involve relevant EMB officials in the process to ensure it can be an exercise in capacity development, and to identify adaptations that the EMB can lead or influence that reduce cybersecurity exposure levels.

Appendix 3 – Literature on Cybersecurity in Elections

The existing resources and knowledge base related to cybersecurity in elections is rapidly expanding.

Below is a list of five recommended 2018 publications which directly address cybersecurity in election processes or related technology, listed by the date of publication:



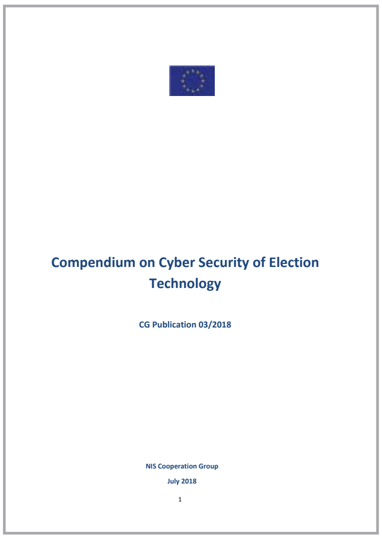
Cybersecurity in Elections

Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies

October 2018

Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies (IFES, October 2018)

This publication from IFES offers a novel methodology to assess threats to cybersecurity and attempt to address them, using a holistic approach. A variant of the HEAT methodology is applied in this playbook and more details are provided in Appendix 2.



Compendium on Cyber Security of Election Technology

CG Publication 03/2018

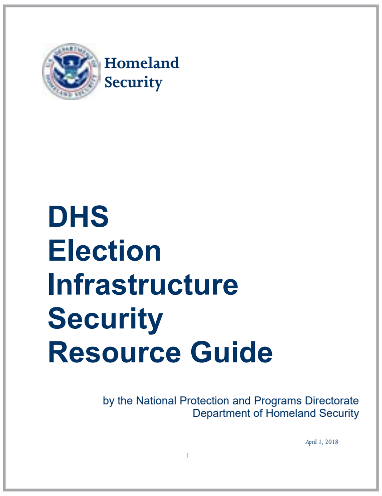
NIS Cooperation Group

July 2018

1

NIS CG Compendium of Cyber Security on Election Technology (July 2018)

The Network and Information Security (NIS) Cooperation group, whidhincludes EC, ENISA and participants from EU member states, has produced a comprehensive compendium of cybersecurity threats in European elections, including the upcoming May 2019 elections for the European Parliament. Specific technical measures to protect elections are considered, related to data integrity and network monitoring, as well as high-level concepts such as accountability, trust and transparency. A variety of examples, including a list of past incidents, are offered as case studies.



Homeland Security

DHS Election Infrastructure Security Resource Guide

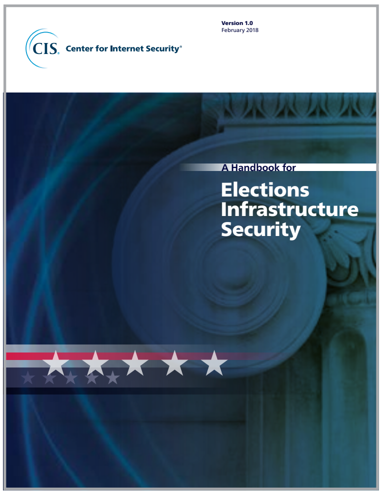
by the National Protection and Programs Directorate
Department of Homeland Security

April 1, 2018

Election Infrastructure Security Resource Guide (by DHS, April 2018)

The U.S. DHS, as a federal security agency, has partnered on a voluntary basis with state- and county-level election authorities to assist in the protection of these de-centralized election systems.

This DHS publication explains what resources are available to election officials in the U.S., and is a cumulative work since early 2017. DHS offers various election-related services and advice, including cybersecurity assessment evaluation of underlying systems, threat detection and prevention of incidents, information exchange as a collaborative effort, and personnel training.



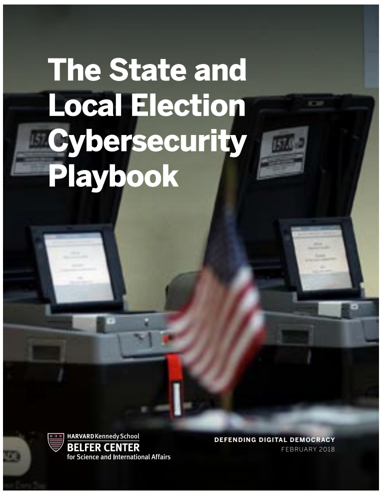
Version 1.0
February 2018

CIS Center for Internet Security

A Handbook for Elections Infrastructure Security

A Handbook for Elections Infrastructure Security (by CIS, February 2018)

The Center for Internet Security (CIS) is a leading non-profit U.S. organization that is active in offering cybersecurity resources both to private and public organizations. Their handbook offers an overview of risks related to various election systems. While it is fine-tuned to consider the election systems that are specific the U.S., most valuable recommendations from the CIS catalog can be employed in any election system in the world. Of note is that these recommendations are very precise and drawn directly from various detailed standards, including the NIST framework and the EAC Voluntary Voting System Guidelines (VVSG).



The State and Local Election Cybersecurity Playbook

HARVARD Kennedy School BELFER CENTER for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Cybersecurity Playbook for Election Officials (by Belfer Center, February 2018)

The Harvard Kennedy School’s Belfer Center for Science and International Affairs established the D3P project back in July 2017 with a direct aim to help defend democratic elections from cyber-attacks and information operations. This playbook considers the cybersecurity aspects as applicable to election jurisdictions throughout the U.S., considering 10 best practices to apply to any election office. Furthermore, technical recommendations address specific election components, including voter registration databases and e-Pollbooks, electronic voting equipment and results reporting systems. As with the CIS Handbook for Elections Infrastructure Security, many of the recommendations are universally applicable.

Appendix 4 – Acronyms

APT – Advanced Persistent Threat

BDS – Breach Detection System

BRIDGE – Building Resources in Democracy, Governance and Elections

BRP – Business Response Plan

CEC – Central Election Commission

CERT – Computer Emergency Response Team

CI – Critical Infrastructure

CIS – Center for Internet Security

CMS – Content Management System

CSIRT – Computer Security Incident Response Team

D3P – Defending Digital Democracy Project

DDOS – Distributed Denial-of-Service

DEC – District Election Commission

DHS – Department of Homeland Security

DMZ – Demilitarized Zone

DPI – Deep Packet Inspection

EAC – Election Assistance Commission

EDR – End Point Response

EMB – Election Management Body

ENISA – European Network and Information Security Agency

EU – European Union

FVL – Final Voter List

GOTV – Get Out to Vote

HEAT – Holistic Exposure and Adaptation Testing

HNEC - High National Election Commission

IAM – Identity and Access Management

ICT – Information and Communication Technologies

IDP – Internally Displaced Person

IFES – International Foundation for Electoral Systems

IPS – Intrusion Prevention System

IT – Information Technology

LAN – Local Area Network

MAC – Media Access Control

MITM – Man-In-The-Middle (attack)

MoI – Ministry of Interior

MoJ – Ministry of Justice

MPLS - Multiprotocol Label Switching

NATO – North Atlantic Treaty Organization

NGO – Non-Governmental Organization

NIC – Network Interface Card

NIS CG – Network and Information Security Cooperation Group

NIST – National Institute of Standards and Technology

ODIHR – Office for Democratic Institutions and Human Rights

OS – Operating System

OWASP – Open Web Application Security Project

PAM – Privileged Access Management

PEC – Precinct Election Commission

PVL – Preliminary Voter List

RAB – Register Administration Body

RMB – Register Maintenance Body

RMS – Results Management System

RRS – Results Reporting System

SCADA - Supervisory Control and Data Acquisition (control system)

SIEM – Security Information and Event Management

SOC – Security Operations Center

SP – Stored Procedures

SPOF – Single Point of Failure

SQL – Structured Query Language

SSSCIP – State Service of Special Communication and Information Protection

SSU – Security Services of Ukraine

SVR – State Voter Register

TCP/IP – Transport Control Protocol / Internet Protocol

TTX – Tabletop Exercise

USB – Universal Serial Bus

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VVSG – Voluntary Voting System Guidelines

WAF – Web Application Firewall

XSS – Cross-Site Scripting