INTERNATIONAL IDEA
INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Cybersecurity in Elections

Models of Interagency Collaboration

INTERNATIONAL IDEA
INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Cybersecurity in Elections

Models of Interagency Collaboration

Sam van der Staak and Peter Wolf

This publication is independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of International IDEA, its Board or its Council members.

International IDEA
Strömsborg
SE–103 34 Stockholm
Sweden
Telephone: +46 8 698 37 00
Email: info@idea.int
Website: <http://www.idea.int>

Design and layout: International IDEA
Cover image: ID 125793633 © Blackboard373 | Dreamstime.com
DOI: <https://doi.org/10.31752/idea.2019.23>

ISBN: 978-91-7671-255-9

Created with Booktype: <https://www.booktype.pro>

Contents

Preface

Information and communication technologies are increasingly prevalent in electoral management and democratic processes. These technologies offer numerous new opportunities, but also new threats. Cybersecurity is currently one of the greatest electoral challenges, even for countries without any form of electronic voting. It involves a broad range of actors, including electoral management bodies, cybersecurity expert bodies and security agencies.

Many countries have found that interagency collaboration is essential for defending elections against digital threats. In recent years significant advances have been made in organizing such collaboration at the domestic and international levels.

This guide tracks how countries are making progress on improving cybersecurity in elections. Based on an extensive collection of 20 case studies from all over the world, it provides lessons for those wanting to strengthen their defences against cyberattacks.

As digital developments affect more of our societies every day, all countries will need to invest in protecting their elections from cyberthreats. We hope this guide will succeed in sharing these cybersecurity experiences with audiences far beyond the countries that had an opportunity to participate in our activities.

International IDEA

Acknowledgements

This Guide was developed in cooperation between the International IDEA's Regional Europe Programme and Global Programme.

Invaluable input, case study interviews and presentations were provided by individuals at a range of institutions, including the Australian Electoral Commission, the Austrian Federal Ministry of Interior, the Central Election Commission of the Republic of Bulgaria, Election Canada, the Ministry of Economic Affairs and the Interior in Denmark, the State Electoral Office of Estonia, the Cybersecurity Branch of the Estonian Information System Authority, the Finnish Legal Register Centre, the Georgian Central Election Commission, the State Chancellery of Latvia, the Central Election Commission of Latvia, the Central Election Commission of Lithuania, the Instituto Nacional Electoral of Mexico, the Central Electoral Commission of the Republic of Moldova, the Dutch Electoral Council, the Permanent Election Authority of Romania, the Independent Election Commission of South Africa, the Swedish Election Authority and the Swedish Civil Contingencies Agency, the Security Service of Ukraine, the UK Electoral Commission, the UK National Cybersecurity Centre and the US Election Assistance Commission.

The Guide benefited from valuable input and suggestions from colleagues at International IDEA, including Therese Pearce Laanela and Adina Trunk, as well as diligent editing and note taking by Alyssa Bittner-Gibbs, Oliver Joseph, Dominika Michalak and Maryam Safi. We also extend our appreciation to Lisa Hagman and Lucy Smith for overseeing the production of this Guide.

Abbreviations

CEC	Central Election Commission
CERT	Computer Emergency Response Team
CSE	Communications Security Establishment
DDoS	Distributed Denial of service
DHS	Department of Homeland Security
DoS	Denial of service
EAC	Electoral Assistance Commission
EMB	Electoral management body
ES	Election Section
ICT	Information and communication technology
IEC	Independent Electoral Commission
INE	National Electoral Institute of Mexico
MoEAI	Ministry of Economic Affairs and the Interior

MoJ	Ministry of Justice
NCSC	National Cybersecurity Centre
NGO	Non-governmental organization
PEA	Permanent Electoral Authority
PEC	Precinct Election Commission
SISA	State Information System Authority
SSSCIP	State Service of Special Communications and Information Protection of Ukraine

Definitions and scope of this document

Cyber-risks refer to any risk of financial loss, disruption or damage to the reputation of an organization due to a failure of its information technology systems. Here the term also includes risks stemming from disinformation about electoral administration and electoral technology that can occur even in the absence of system failures.

Cybersecurity relates to protecting Internet-connected systems, networks, software and data from unauthorized access or exploitation. It is also used here to include the security of offline election technologies and protecting the integrity of the electoral process from disinformation and influence operations.

Cyberthreats in elections include threats to all possible technology based on hostile and/or illegal acts designed to undermine the integrity of the electoral process.

Interagency collaboration is used here to indicate collaboration designed to prevent and mitigate cyber-risks and respond to cyber-related incidents in elections. Such collaboration is not necessarily limited to government agencies; it also includes a broad range of actors, including EMBs, media and social media providers, political parties, electoral candidates, civil society and other electoral stakeholders, as well as private sector actors including election technology providers and consultants.

Vulnerabilities are weaknesses in the electoral process that make it prone to successful or alleged attacks. Such weaknesses can include the technology (devices, software, networks) itself as well as inadequate procedures and human factors such as poorly trained staff.

The scope of this publication focuses on cyber-risks and threats in electoral processes that fall within the responsibility of an EMB. This includes a broad range of possible attacks against the confidentiality, integrity and availability of election-related data and technology. For social media and other forms of online publications, this includes spreading disinformation about the electoral process.

1. Introduction

Some countries such as Estonia, Georgia or the Ukraine have already been exposed to cybersecurity threats to their electoral process for 10 years and more. However, it was only the widely debated cyber-related incidents that are thought to have influenced the 2016 US presidential elections that created broader awareness and attention of this topic. Within several months, this led to worldwide discussions on how to counter increasingly prominent risks of cyberattacks on elections and democracy in both young and established democracies.

Elections rely on varying combinations of manual and technology-based procedures. As neither truly unhackable technology nor entirely tamper-proof manual processes exist, an essential task in election administration involves the management and mitigation of manipulation risks through a range of integrity, audit and control measures. While countries around the world have long-standing best practices for integrity measures for paper-based and manual processes, recent events have highlighted the need to address the risks that emerge from the ever-increasing use of technology in elections.

A common misperception is that only countries with electronic voting or other high-profile election technologies are at risk of a cyberattack. However, all elections depend on information and communication technology (ICT) tools, from voter registration to an electoral management body's (EMB's) website. Therefore, while the type of cyber-risks, adversaries and attack vectors vary between countries, EMBs—as well as high-level office holders, security agencies and democracy assistance providers—now agree on the need to invest more in understanding, preventing and mitigating the risks that new technologies bring to democratic processes and elections.

A second misperception is that an EMB is the main (or even sole) agency responsible for cybersecurity in elections. However, cyberthreats against elections and democracy arise in a variety of forms that fall under the jurisdiction of many different actors:

- cyberattacks against election-related infrastructure aimed at breaching the confidentiality, integrity and availability of election technology and data;
- disinformation campaigns that attempt to undermine the credibility of the electoral administration and democratic institutions;
- cyberattacks against electoral stakeholders, parties, candidates, media and campaigns; and
- disinformation campaigns designed to shape the political debate.

Addressing these cyberthreats often requires more than the implementation of technical mitigation measures by the EMB or any other single entity.

EMBs are commonly responsible for protecting the integrity of their own systems and for upholding the trust and credibility of their institution. Hacking attacks against electoral stakeholders, such as political parties and candidates, and undue influence over the political debate are more commonly a grey area over which other state agencies have jurisdiction; alternatively, there may be no regulation and/or clear mandate for countermeasures.

Election managers and stakeholders often have neither the resources nor the expertise to defend themselves from sophisticated cyberthreats. Cybersecurity expert bodies generally have limited electoral expertise, and may not always give high priority to defending against election-related threats. They may instead focus on protecting critical infrastructure such as the military, public utilities or high-level economic targets from cyberattacks.

Therefore, more interagency collaboration is needed to pool the required resources and expertise; for developing a better mutual understanding of areas of responsibility, overlaps, gaps and points of contact; and for building holistic defences against both domestic and international cyberattacks on elections and democracy.

This publication describes emerging models of interagency collaboration, at the behest of many election professionals who indicated a need for such a resource. It follows a number of International IDEA events and interviews related to cybersecurity in elections that have taken place following a first international round table on cybersecurity in elections (Wolf 2017), in which representatives of electoral commissions, security agencies, and parliamentary and independent experts have discussed ways to counter real and perceived risks of hacking in elections.

It explores several questions raised as part of a broad needs assessment exercise:

- What election-related technologies create exposure to cyberthreats?
- Why are cyberthreats important even for countries that do not use e-voting or similar high-profile election technologies?
- Which government bodies and private sector companies need to be involved?
- How should the collaboration of the various actors be structured, and what are their respective roles and responsibilities?
- What formal frameworks—from legislation to memoranda of understanding—are required to enable, encourage and facilitate interagency cooperation?
- Which measures need to be taken, and in which part of the electoral cycle?
- Elections as critical national infrastructure: what does this assessment entail for the EMB?

The publication is based on 20 case studies with EMBs and related government agencies as well as a round-table discussion held in 2018 that facilitated the exchange of experiences between countries as diverse as Austria, Australia, Belgium, Bulgaria, Canada, Denmark, Estonia, Finland, Georgia, Latvia, Lithuania, Mexico, Moldova, the Netherlands, Norway, Romania, South Africa, Sweden, Ukraine, the United Kingdom and the United States.

2. Cyberthreats throughout the electoral cycle

Cyberthreats can undermine electoral integrity by either exploiting technical vulnerabilities or creating the perception that such vulnerabilities exist. Cyberthreats fall broadly into two categories: (a) attacks targeting election-related technologies; and (b) disinformation campaigns targeting the perceived integrity of the electoral process.

2.1. Attacks targeting election-related technologies

The main targets of hacking attacks against election-related technology include voter registration technologies, voting, vote counting technologies, result transmission and aggregation technologies, websites for result publication and other online election-related services, institutional and private email accounts and communication systems, and broader national infrastructure, including e-government systems, power grid and communication links.

Hacking attacks against the electoral process can be either generic or election specific. Electoral stakeholders may therefore become either random victims or intentional targets of attacks. Generic attacks often require little sophistication and limited resources and include Denial of Service (DoS) attacks, website breaches, and malware and ransomware attacks.

DoS attacks involve flooding online resources with so many requests that the service becomes very slow or completely unavailable. Such attacks do not penetrate the attacked systems, and cannot change data or access confidential information. The damage is caused by making the systems unavailable, which has reputational implications for the attacked institution. DoS attacks can target websites to make them inaccessible, or communication systems to make communication for their users difficult or impossible. For instance, they could create disruptions by blocking and overloading mobile phones and the communication channels and devices of key election staff (see Box 2.1). If DoS attacks come from a single source, then this source can usually be blocked easily. Distributed Denial of Service (DDoS) attacks are more difficult to defend against, as they come from many different sources; significant computing resources and cooperation with technology partners and Internet providers are required to combat such attacks. As they are relatively simple to execute, successful or attempted DDoS attacks are arguably the most common type of cyberattack; virtually all EMBs experience them at some point. Therefore, many EMBs have recently put in place safeguards to protect against or adequately respond to them.

Box 2.1. Indonesia: cyberattacks against election commission staff

During Indonesia's 2018 regional elections, there were attempts to hack the results data web page of the General Elections Commission, as well as the Telegram and WhatsApp accounts of key election administration staff via weaknesses in the mobile text messaging systems. The attempts sought to gain access to and block the usage of those services in order to disrupt the election process.

Website breaches involve defacing the appearance of websites or manipulating their content. Changing the visual appearance is usually very obvious and aims to cause reputational damage. Content manipulation can be more subtle; such attacks may aim to create confusion, for example by presenting misleading information or altered election results. Such website breaches are based on exploiting the vulnerabilities of a public website and gaining access to a public web server, but often do not impact any internal information technology (IT) systems or lead to the manipulation of the internal data of the attacked institution. However, successful attacks do cause uncertainty and undermine the credibility of the institution. Breaches of election websites can also lead to the leaking of personal data when online voter registers are compromised.

Box 2.2. Ukraine: A long history of attacks against the Central Election Commission's online infrastructure

A series of simultaneous cyberattacks took place during Ukraine's 2014 presidential and parliamentary elections. The attacks disrupted the transmission of results by district electoral commissions, in part by launching DDoS and defacing attacks against the website that displayed the election results; malware and phishing attacks also took place. A similar DDoS attack against the Central Election Commission and candidates was launched a few weeks ahead of the 2019 presidential election. However, the 2019 cyberattacks did not succeed in disrupting the results because the election commission had installed appropriate defence mechanisms.

Malware and ransomware attacks can have adverse impacts on elections by making essential systems and data inaccessible (see Box 2.3). They are not necessarily politically motivated; electoral stakeholders can also become random targets of criminally or financially motivated hacking. In recent years, 12 per cent of global cyberthreat activity affecting democratic processes was criminally, rather than politically, motivated (CSE 2019).

Box 2.3. North Macedonia: ransomware attack against the State Election Commission

About one month before the 2019 North Macedonian presidential election, the State Election Commission's key information and communication systems did not function properly, which affected the timely accessibility of information; the publication of session minutes, instructions and decisions; the online verification of voters' data in the voter register; and the online register of complaints. This raised questions related to the commission's ICT security. According to the election commission, systems affected by the ransomware GEFEST 3.0 included the file and email servers, which also impacted the accessibility of the voter register and the database of public employees used to appoint the Electoral Boards (OSCE/ODIHR 2019).

More advanced attacks explicitly aim to access internal systems, private data and information. Manipulating such data is often more difficult than attacking online public resources. Internal systems are usually much better protected and are not directly accessible from the Internet. Successful attacks are the result of either severe ICT security shortcomings or advanced persistent threats, which are well-planned, multi-phased and commonly conducted by a well-resourced adversary, frequently a nation state; these attacks can cause widespread and severe damage. The attacker selects a very specific, often personal, target and uses the most sophisticated available techniques, including publicly unknown vulnerabilities ('zero-day exploits'). Advanced persistent threats are executed over long periods of time until they eventually succeed; they can even target systems that are not connected through the Internet, for example though infected USB sticks and devices.

In organizations with low technical vulnerabilities, eliciting access credentials through social engineering is often the easiest and most successful attack vector. Social engineering includes exploiting human psychology to gain access to systems and data and to elicit passwords and other access credentials from users. It can be applied through direct, personal contacts or more commonly through phone calls and phishing and spear phishing emails that lure recipients to reveal confidential information or to click on links to compromised websites that serve as the starting point for further hacking and malware attacks.

Finally, insider attacks include intentional data and system breaches by users with access to election-related information systems. Usually such advanced and targeted attacks can only manipulate result transfer and aggregation systems and election-related online services—such as online voter, party or candidate registration systems—and publicly accessible election-related devices where technology such as voting machines or voter identification systems is used in polling stations.

2.2. Vulnerabilities

Generic cyberattacks exploit vulnerabilities including a lack of 'cyberhygiene'. This term refers to (a) users' degree of training and awareness on how to maintain the system's health and online security; (b) how up to date the organization's technology is, including the conduct of regular testing and maintenance; (c) whether the procedures and security principles are adequate to address new and evolving cyberthreats; (d) whether there is sufficient separation between internal and online connected systems; (e) whether staff with access to confidential systems are sufficiently screened and monitored, to reduce the risk of insider attacks; and (f) whether the organization's cybersecurity measures can defend against the resources and ambitions of a dedicated attacker (see Box 2.4).

Box 2.4. Romania: cyberhygiene training for political parties

The Romanian Permanent Election Commission introduced cyberhygiene training programmes for political parties to protect parties' internal information as well as the election-related data the commission provides to parties. This is because any hacks and data leaks from parties would also create the perception of a successful hack against the election commission.

Some vulnerabilities specific to the nature of the electoral processes pose additional cyber-risks compared to other governmental tasks. The periodic nature of elections results in election-related databases and technology being used periodically and reactivated and scaled up around election day. This makes continuous monitoring and management of cyber-risks much more difficult than in other domains. Election day is the 'single point of failure' for elections technology. Many systems, and particularly government IT systems, are designed to be unavailable for a few hours or even days as the result of severe cyberattacks. Election technology must be operational on election day, so an adversary merely needs to create interruptions or confusion for a few hours during the critical period around elections to achieve maximum damage.

Election technology that is used by millions of citizens only once every few years must be easily accessible and secure. These two principles are often contradictory but need to be carefully balanced. Multiple government bodies may share responsibility for complex election-related procedures, such as voter registration, which may leave gaps open for exploitation. If the roles and responsibilities of each actor are not clear, no agency may have ultimate responsible for cybersecurity. Limited financial and human resources and limited IT competence at EMBs for developing and maintaining election technologies can yield poorly designed or secured systems and procedures.

The supply chain of election technology can be another source of vulnerability to cyberattacks. Where custom election technology is sourced, in some cases from foreign vendors, there may be concerns that systems may, whether intentionally or not, be delivered with malware or vulnerabilities.

2.3. Disinformation targeting the perceived integrity of the electoral process

Disinformation is deliberately—often covertly—spreading false, misleading or inaccurate information with the intent to cause harm by influencing public opinion. Disinformation in elections can be spread by either domestic or international actors. Foreign actors may use disinformation as part of 'influence' (or 'information') operations, a discipline traditionally used in military contexts that has been increasingly applied to elections. Such operations often exaggerate and misrepresent publicly known and debated issues. EMBs' mandate only entails countermeasures against disinformation campaigns if they specifically concern the electoral process and its administration.

Disinformation activities as part of a political campaign are outside the scope of this document, as they are usually outside the authority of the election administration (see Box 2.5). In this domain, debates about the right level of regulation and legislation, self-regulation and codes of conduct are still ongoing, as this requires a careful balance between preventing disinformation campaigns and protecting the freedom of speech, as well as distinguishing between illegal online activities and legitimate online campaigning. As of 2019, only a few countries have specific 'fake news' legislation in place or have discussed related bills (Poynter Institute 2018).

Box 2.5. Latvia: hack of domestic social media and the role of the disinformation task force

A popular Latvian social network site called Draugiem was hacked on the day of the 6 October 2018 general election. A statement in Russian appeared, saying 'Comrades Latvians, this concerns you. The borders of Russia have no end', and was accompanied by images of Russian soldiers in Crimea and Russian military parades in Moscow. The source of the hack was not clear.

Since Draugiem is privately owned, no formal response from state institutions was required. However, Latvia's disinformation task force felt it was important to ensure the media reported on the incident in a balanced way to avoid a negative public perception of the electoral process. The task force therefore responded in three ways: (a) it asked the cyberagency response team to immediately investigate the hack; (b) it publicly announced that the hack in no way affected the elections; and (c) it communicated upwards to political decision-makers on the risk level, to ensure a measured political response. As a result, the response by traditional media and the public was measured, and the prevailing sentiment was that the country's electoral system is safe.

Two types of information operations are particularly relevant to EMBs, since they attempt to influence elections. Such operations often utilize online and social media mechanisms to reach voters. First, disinformation can seek to suppress voter turnout, for example through false claims that polling stations are closed or that elections are delayed due to weather, violence and other factors, or claims that votes can be cast online or by telephone where this is not the case (see Box 2.6).

Box 2.6. Canada: domestic threats

In 2011, Canada experienced the Robocall scandal, in which thousands of voters in almost 250 ridings (constituencies) across the country reported receiving automated phone messages falsely telling them that their polling stations had been changed. This information operation aimed to suppress voter turnout. Elections Canada's investigations found that domestic political actors were responsible. The incident prompted Elections Canada to set up an Electoral Integrity Office to identify domestic and international cyberthreats, assess risks and set up systems to track and prevent cyberattacks by foreign actors, political operatives or individuals who might want to disrupt elections or manipulate the results.

Second, disinformation can also aim to undermine trust in electoral processes, institutions and technologies by spreading rumours of manipulation and malfeasance. Where perceptions of electoral integrity are traditionally high, even pointing to small shortcomings may seriously damage this perception (see Box 2.7).

Box 2.7. Mexico: disinformation about the electoral process

Verificado, a fact-checking initiative for the 2018 elections in Mexico, identified several false claims against the election administration and the electoral process (Verificado 2018). These included misleading instructions on how to mark ballots that sought to invalidate votes, rumours about rules allowing individuals to vote on behalf of deceased relatives, and rumours about inadequate or breached ballot security. National Electoral Institute agreements with technology contractors to protect the election infrastructure against hacking attempts were even misinterpreted as transferring control of the official results system to these private companies and their owners.

Election technologies can become easy targets of disinformation when the public and electoral stakeholders do not fully understand their details. Such disinformation can include unfounded rumours that election technology is insecure and hackable (or has been hacked), exaggeration of minor technical weaknesses and breaches, and other intentional misrepresentation of facts. Creating such perceived cybersecurity risks can potentially be as disruptive as actual cyber interference (see Box 2.8).

Box 2.8. The Netherlands: seeking interagency collaboration when the public is watching

In 2006, the Netherlands was forced to abandon electronic voting just weeks before the general elections after a Dutch white hat hacker group advocating against electronic voting had demonstrated the security risks of the country's voting computers. Since then, election authorities in the Netherlands have been fighting an uphill battle over the use of any electronic instruments in elections, even after returning to manual voting and counting. In 2017, white hat hackers again claimed that the software that municipalities used to aggregate and calculate election results was insufficiently protected. This led the Minister of the Interior to ban the software two weeks before the elections, despite protests from the electoral commission and municipalities. The episode illustrates the difficulty of maintaining interagency collaboration in the public spotlight.

Overly ambitious, undeliverable election technology projects demanded by electoral stakeholders can lead to undue public expectations. This may prompt parties to wage information battles about the real or perceived strength of the country's cybersecurity measures. Any poorly implemented or understood election technology can be instrumentalized to deliberately undermine the credibility of an election, and can make the timely conduct of elections impossible due to financial, time or technical constraints.

Attacks designed to leak electoral stakeholders' confidential information constitute a combination of hacking attacks and influencing operations. EMBs need to be especially aware of the risk of data leaks from stakeholders who have privileged access to election data such as voter registers and/or incomplete election results. Guarding against such election data leaks is one possible area of interagency cooperation and joint counter measures by EMBs, other government agencies and electoral stakeholders.

Table 2.1. Spectrum of election-related cyberthreats

Generic cyberattacks—electoral process may be random target	Targeted cyberattacks against the electoral process	Exploitation of election-specific vulnerabilities	Disinformation/operations against perceptions of electoral integrity
DoS attacks	Zero-day exploits	Periodic nature of elections	Leaking of confidential information
Defacing websites, manipulating website content	Social engineering, phishing	Election day as single point of failure	Disinformation about election technologies
Criminally or financially motivated generic hacking	Access and manipulate election data	Used only once every few years, but by millions of users	Disinformation about the electoral process
Exploiting a lack of cyberhygiene, e.g. through 'cracking' weak passwords	Hacking of election technology	Limited resources to maintain election technology	Undeliverable election technology projects
	Insider attacks	Complex procedures, often shared between different agencies	Disinformation as part of the political campaign

2.4. Adversaries

In the aftermath of the 2016 US election, many countries perceive foreign states that seek to influence national elections as the main adversaries to cybersecurity in elections. International law also applies within cyberspace; election hacking is legally considered an 'internationally wrongful act' and a breach of sovereignty that requires the victim to respond. However, attribution and obtaining proof that perpetrators are the organs of a foreign state are very challenging. A range of other adversaries may seek to utilize technology to influence election outcomes, including domestic political actors as part of an election campaign, hacktivists who promote a political agenda or social change via hacking activities, including a demonstration of their lack of confidence in existing election technologies, and terrorists resorting to cyberoperations.

Adversaries outside the political spectrum include organized crime groups trying to influence elections, cyber criminals attacking systems for financial gain, and individuals and groups that attack systems to demonstrate their skills and gain fame and notoriety.

Depending on their motivation and willingness to resort to illegal methods, computer hackers are often categorized into three groups. Black hat hackers with malicious intent conduct operations for their own gain and to damage their targets. White hat hackers are ethically motivated and operate legally; they are frequently contracted to test systems in order to discover security flaws so they may be addressed. White hat hackers do not exploit or publish weaknesses they uncover before any vulnerabilities are addressed. Grey hat hackers may occasionally break the law, but do not exploit the vulnerabilities they uncover.

Any type of hacker can negatively impact the integrity of elections. Even well-intentioned white hat hackers can cause considerable damage to electoral integrity if they carelessly and irresponsibly publish their findings, such as doing so too close to an election with insufficient time to fix flaws or by exaggerating the severity of discovered weaknesses to garner increased publicity. Hacking events such as the DefCon Voting Village (DefCon 2017; DefCon 2018) in the USA serve as an opportunity to advocate improved election technology, but can also threaten the credibility of elections.

Table 2.2. Adversaries that can negatively impact the integrity of elections

Politically motivated	Not politically motivated
Foreign nation states	Organized crime
Domestic political actors	Financially motivated criminals
Hacktivists	Individuals
Terrorists	

2.5. Mitigation measures

While a detailed account of measures to mitigate cyber-risks goes beyond the scope of this publication, they usually include the following measures.

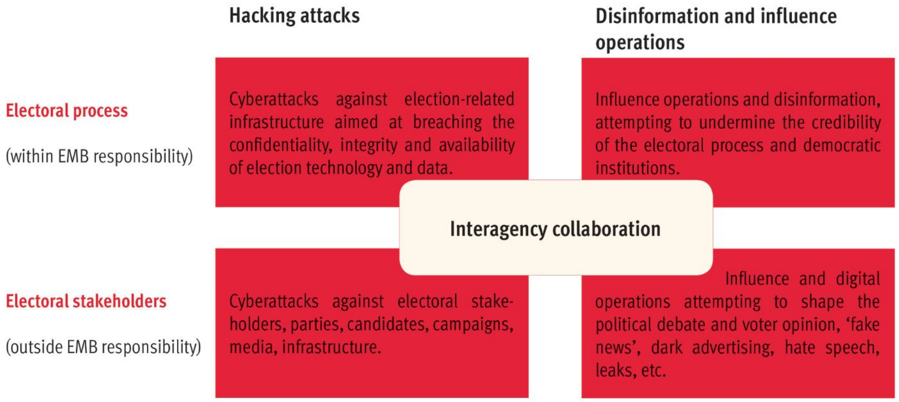
- *Securing technology* through regular reviews, audits and updates of technology and procedures, which are reinforced with redundant and backup systems. These include securing alternative communication channels for disseminating information, state-of-the-art encryption and identification systems, ‘air gapping’ and isolating critical technology from the Internet as far as possible, and 24/7 monitoring of all critical infrastructure.
- *Quality control and audits* of election procedures at different levels, incorporating redundancies in critical processes including double data entry, paper or telephone-based verification. Efforts are made to ensure the implementation of such procedures.

- *Managing cybersecurity in the supply chain*, including the scrutiny and careful selection of trusted suppliers and vendors.
- *Investing in human resources*, staff training and cyberhygiene, clearly assigning staff roles and responsibilities, adopting a 'four eyes principle' to make sure critical processes are never executed by a lone staff member, and including background screenings of key election staff with administrative access.
- *Monitoring online conversations* on public social media, but also on the dark web, hacktivism forums and other resources for clues of data leaks or planned coordinated attacks.
- *Establishing criminal liability* under the law for election malpractice and manipulation, and prosecuting identified lawbreakers.
- *Continuous collaboration* by maintaining contact with a multitude of actors and establishing internal and public communication early and long before any crisis surfaces.

2.6. The need for interagency collaboration

While adversaries are free to choose any attack vector, defence strategies are much more fragmented. Depending on the country context, some cyberthreats fall under the mandate of various levels of election administration, other threats are the responsibility of other state agencies, some are countered mostly through private sector or political party action and industry self-regulation and some—especially where technical progress is fast or freedom of speech may be at stake—are not regulated at all. The ensuing network of jurisdictions, competences and responsibilities is what makes a whole of government approach and interagency collaboration on cybersecurity in elections essential.

Figure 2.1. Cyber-risks in elections vs. EMB mandate



	Hacking attacks	Disinformation and influence operations
Electoral process (within EMB responsibility)	Cyberattacks against election-related infrastructure aimed at breaching the confidentiality, integrity and availability of election technology and data.	Influence operations and disinformation, attempting to undermine the credibility of the electoral process and democratic institutions.
Electoral stakeholders (outside EMB responsibility)	Cyberattacks against electoral stakeholders, parties, candidates, campaigns, media, infrastructure.	Influence and digital operations attempting to shape the political debate and voter opinion, ‘fake news’, dark advertising, hate speech, leaks, etc.

Interagency collaboration

3. Models of interagency collaboration

The form of interagency collaboration analysed in the case studies in this publication depends on four primary factors: (a) the number and type of agencies involved; (b) forums for interagency collaboration; (c) cooperation between different levels of the EMB; and (d) collaborating with non-state agencies. This chapter discusses each factor in turn.

3.1. Number and type of agencies involved

In some countries interagency collaboration is limited to a few agencies, but across the case studies a large number of agencies were identified as potential collaboration partners (see Table 3.1). Collaboration can be limited to government agencies, but it often includes non-state actors, civil society, media, political parties and candidates, as well as the private sector (see Box 3.1). Depending on the country context, the EMB can serve as either a mediator or a driver of collaboration.

Box 3.1. Moldova: close collaboration with security agencies during cyberincidents

In 2014, Moldova introduced a digital voter register, which records voters' presence at polling stations, as an additional verification mechanism. When it was first used during the 2014 general election, the system unexpectedly went down for several hours. Although the breakdown was due to insufficient server backup, rumours soon spread that an attack had taken place. The Central Election Commission's newly established collaboration with the security services, however, quickly paid off. They rapidly provided additional servers to the election commission's headquarters, and publicly renounced rumours of an attack. These actions quickly returned the election to the commission's control and established the foundations for interagency trust.

Table 3.1. Agencies potentially involved in collaboration on cybersecurity

Government sector	Non-government sector
Government executive office (cabinet/prime minister's/president's office)	Print and broadcast media
Various levels of election administration	Social media providers
Dedicated IT security teams within the election administration	Political parties and candidates
Administrative bodies responsible for voter registration (if different from EMB)	Academia
Cybersecurity expert bodies (e.g. Computer Emergency Response Team, Cybersecurity Centre, Information System Authorities)	Private sector ICT contractors
State e-government agencies	Private sector security contractors
State enterprises providing election technologies	Utility and infrastructure providers
Trust service providers for digital identity	White hat hackers
Ministries: Interior, Justice, Communication, Defence, Foreign Affairs	
Public security agencies	
Police forces at various levels	
Intelligence and national security agencies	
Public prosecutor	

3.2. Dedicated forums and administrative bodies

Some countries organize interagency collaboration through dedicated forums such as task forces, working groups, dedicated projects and administrative bodies (see Table 3.2). Some task forces meet on an ad hoc basis, while others conduct regular forums in order to exchange information. Many countries have a single task force on election cybersecurity, yet Estonia has found that a model with several small, focused groups is more effective. The USA maintains two forums—one for collaboration between state agencies and one for collaboration with the private sector.

Table 3.2. Examples of interagency forums on cybersecurity

Country	Cybersecurity in elections forum
Australia	Electoral Integrity Task Force
Bulgaria	Interservice group under the prime minister CEC/Ministry of Interior joint teams for fight against electoral crimes
Canada	Election Integrity Office
Denmark	Inter-ministerial task force
Estonia	Weekly ICT working group Weekly public relations working group Working groups for registries, voting cards, voter rolls Voting from abroad task force Internet voting task force
Georgia	CEC joint working group
Latvia	Cybersecurity in Elections working group Disinformation task force
Moldova	Joint services working group
Sweden	Counterinfluence project coordinated by the Civil Contingency Agency
Ukraine	EMB/Security Service Joint Commission on Cybersecurity
United States	Elections Government Sector Coordinating Council Sector Coordinating Council

3.3. Cooperation between different levels of the EMB

Countries with a centralized EMB that is responsible for organizing elections at all levels, including polling stations, usually find it easier to apply uniform cybersecurity measures throughout the country. In countries with a decentralized model, where independent, local EMBs have direct operational control over organizing elections, yet the general public (and sometimes even politicians) tend to hold the central election authority ultimately responsible for any local incidents. The central authority regularly receives the brunt of criticism and reputational damage for any errors.

Decentralized EMBs therefore require new and intensified cooperation and support between their different levels. There may also be a need to mitigate misgivings or hostility regarding national-level oversight in local affairs. In such a decentralized context, a key role of interagency collaboration is often coordination and trust building between local election administrations and a range of state-level agencies, from the national EMB to security agencies.

3.4. Cooperation with non-state agencies

The private sector, which includes election-related technology and telecom providers as well as risk analysts, is an important collaboration partner for most EMBs to secure technology, conduct security audits, and propose and support the implementation of countermeasures. Some countries include utility providers in their interagency collaboration process in order to minimize the risk of service interruptions around election day.

Contacts with media outlets—and increasingly social media providers—are important to ensure that communication plans can be executed even during an attack. The case study interviews conducted for this publication revealed that the level of cooperation with social media providers varies greatly between countries. Some EMBs largely refrain from social media activities, while others, such as Mexico, have formal memoranda of understanding in place. Currently, the ability and willingness to cooperate with social media providers varies among larger countries with well-established cooperation and services, and is unavailable in smaller countries or less important markets.

Political parties and candidates are targeted in election hacking attacks not only due to their perceived value as a target, but also because they are often the weakest link of all electoral stakeholders. This is especially true where there are a large number of parties, and insufficient resources to invest in technology security. The degree to which it is possible and appropriate for an EMB or other state agency to provide cyber-related advice to political parties varies greatly between countries. However, it is recommended to inform parties of the potential havoc of cyberattacks alongside the scope of support that EMBs and other agencies can offer in the event of such attacks. When political parties receive privileged access to election data, such as voter lists or preliminary results, this also indicates a need for related instructions and conditions on how to protect this data.

Academia plays an important role in electoral cybersecurity. For instance, technology experts or hacktivists may warn stakeholders of the danger of not taking ICT security in elections seriously. These academics and others provide a wide range of input including suggestions on how to improve systems and publicly demonstrating genuine vulnerabilities in the current electoral setup, both technological and integral. Building a constructive relationship with such experts, provided their intentions and modes of operation are transparent, can help improve systems and lower the risks of negative publicity. Some academic institutions have initiated cybersecurity-related collaboration with electoral administrators and support electoral stakeholders based on their research. For instance, Harvard Kennedy School's Belfer Center for Science and International Affairs (2018a, 2018b) created *The Cybersecurity Campaign Playbook*. Likewise, the annual US-based hackers conference DefCon has focused on electoral cybersecurity and produced the *Voting Machine Hacking Village Report on Cyber Vulnerabilities in the U.S.* (DefCon 2017; DefCon 2018). In Latin American countries such as Mexico and Venezuela, academic institutions serve on an independent election technology review and audit body that facilitates technology improvement and strengthens public trust. Finally, in Indonesia, academics play an important role in developing election-related technology.

4. Operationalizing interagency collaboration

As part of a more comprehensive government approach to cybersecurity in elections, the key goals of interagency collaboration commonly include: protecting the confidentiality of election-related private data such as voter rolls, emails and internal documents; safeguarding the availability and integrity of election-related technology; protecting the integrity of elections against disinformation campaigns; securing resources, expertise, funding, and institutional and legal backing for the required measures; and strengthening the cybersecurity of electoral stakeholders.

4.1. Focus areas

Specific focus areas of collaboration can include:

1. *Organizing interagency communication,* starting with compiling a directory of interlocutors and emergency contacts at participating agencies, followed by broad agreements regarding the role, coordination and leadership between these agencies. To reinforce these partnerships, agencies should regularly utilize channels of communication between agencies, including the creation of task forces, working groups and similar collaborative forums. Creating working relationships and building confidence between participating agencies, and overcoming differences between institutional cultures, are just as important as substantive cooperation.

2. *Joint risk assessment and situational awareness* through a multi-agency led assessment of cyber-risks that includes information exchange, situation reports and the development of a shared understanding of vulnerabilities and how they evolve during and between elections (see Box 4.1). Coordinated media and social media monitoring as well as intelligence sharing by relevant agencies can provide further important inputs.

Box 4.1. Finland: intelligence sharing and situational awareness

Finland's Legal Register Centre meets at irregular intervals with various agencies. Cybersecurity is only one of the topics covered in these election-related coordination meetings, which establish a continuously updated risk overview and specify appropriate mitigation measures based on threat assessments and intelligence. Cyber-risks are assessed on an ongoing basis and for each election, taking into account recent international developments.

3. *Coordinating public communication and providing voter information* is a key area of comprehensive protection against cyberthreats. Since actual threats are as relevant as perceived threats, a consistent and coordinated public communication strategy is needed. Public communication should aim to inform voters prior to an election, including by providing accurate and consistent messaging following any incidents.

   The agencies included in this publication vary widely in their communication approaches. Some countries prefer not to give this topic heightened visibility to avoid increasing citizens' unease, while in others, citizen awareness and a well-informed electorate are seen as the best defence. Regardless of the level of public communication, all related agencies should develop a joint communication strategy and share a common message about threats and countermeasures before (or during) a possible crisis.

   To disseminate important messages in a timely manner, efficient communication channels must be established with the media. This increasingly includes formalized agreements with key social media providers to provide voter information and to make sure disinformation about the electoral process is promptly rectified, including through highly visible announcements from the EMB if needed. For example, in 2018 Mexico's EMB concluded memoranda of understanding with Twitter and Facebook (INE 2018; *El Universal* 2018).

4. *Creating prevention and response mechanisms* based on the established risks. Electoral stakeholders can be supported and advised on preventive measures to protect and mitigate these risks, and to help form contingency plans in case cyberattacks do occur. This may include protocols that stipulate when an EMB escalates incidents to security agencies or political decision-makers. Fast responses to emerging issues, including the efficient adjudication of complaints, are essential to maintaining public trust.

Box 4.2. Estonia: maintaining trust in a highly digitized society

Although Estonia has among the highest levels of digital democracy in the world, its EMB does not consider technology breaches to be a major threat. The country's small size helps: with only 1.3 million inhabitants, it is relatively easy for Estonian EMB staff to find counterparts from other agencies who can help secure election-related technologies. The EMB considers it more important to maintain its strict political impartiality in order to ensure political parties' support and voters' confidence in electronic voting, and to help electoral candidates and young voters use digital technologies responsibly. In a highly digitized society, public trust forms the foundation of cybersecurity.

5. *Developing and providing expertise, tools and resources* on cybersecurity, including training programmes and guidelines such as the EU Compendium on Cybersecurity in Elections (NIS Cooperation Group 2018) or the US Election Assistance Commission's resources on *Election Security Preparedness* (US EAC n.d.).
6. *Providing independent assessments and certifications* of security measures implemented by the EMB through another state agency (see Box 4.3).

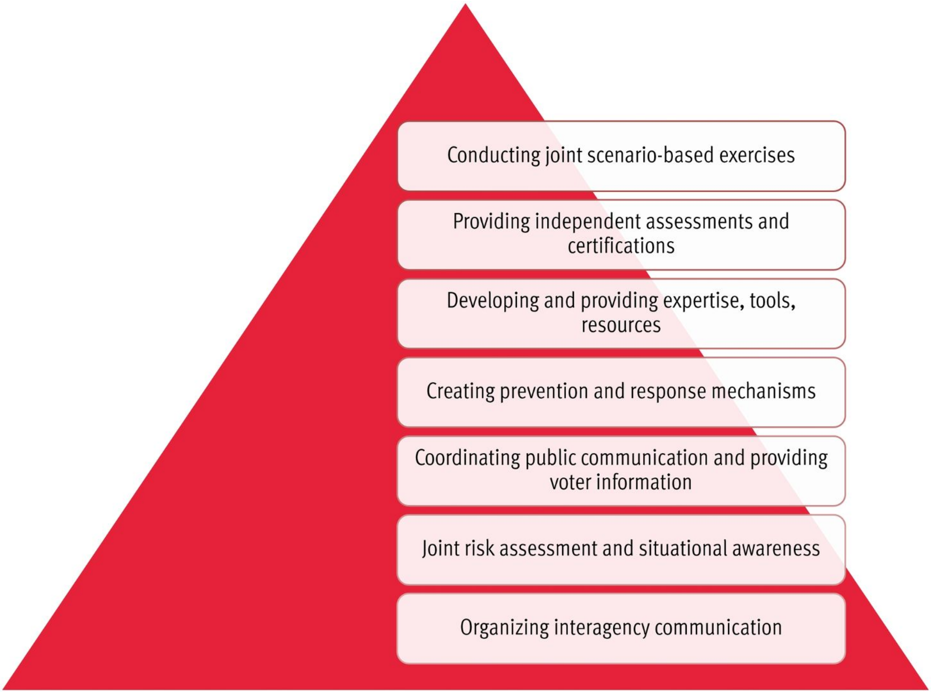
Box 4.3. Ukraine: collaboration between the Central Election Commission and other authorities in certification and monitoring election ICTs

All election-related information systems must undergo state assessment to receive a certificate of compliance before they can be used by the Central Election Commission. The State Service of Special Communications and Information Protection of Ukraine tests the system and assesses its conformity with the terms of reference and information protection requirements. During the operation of these information systems, experts from this agency monitor and protect them from attacks.

7. *Conducting scenarios-based joint exercises* is a more advanced form of interagency collaboration that only some surveyed countries have in place. These crisis scenario simulations are conducted to test the efficiency of a country's response capabilities. They are designed to get the relevant agencies to work together cooperatively in response to potential crises, to identify planning and procedural shortcomings, and to collect feedback for further improvement. Tabletop exercises, in which participants discuss their roles and responsibilities in various scenarios, are more cost effective and therefore more commonplace than full-scale real-life simulations of incidents.

Interagency collaboration happens at various levels that mutually build on each other, indicating a progression towards more comprehensive collaboration (see Figure 4.1).

Figure 4.1. Levels of interagency collaboration


Conducting joint scenario-based exercises
Providing independent assessments and certifications
Developing and providing expertise, tools, resources
Creating prevention and response mechanisms
Coordinating public communication and providing voter information
Joint risk assessment and situational awareness
Organizing interagency communication

4.2. Setting up and facilitating interagency collaboration

The case study interviews conducted for this publication indicate that many countries are still constructing measures to protect elections against cyberthreats. While they increasingly recognize the importance of interagency collaboration, many are still in the early stages of setting up and utilizing the required mechanisms.

4.2.1. Challenges and limitations

Typical challenges to interagency collaboration include contrasting institutional cultures, especially between EMBs and security services, and therefore a hesitation to collaborate on all sides (see Box 4.4).

Box 4.4. Finland: overcoming cultural barriers between agencies

Working with non-traditional agencies can require as much of an organizational shift as a cultural or even linguistic one. In Finland, the military and security services traditionally consider only military targets to qualify as 'critical infrastructure' and therefore require their involvement. When the country decided not to use online voting in 2017 for security reasons, these agencies decided elections no longer fell within their responsibility. Despite the intrinsic cultural barriers between agencies, the Legal Register Centre, the technical arm of the Finnish EMB, reached out to security sector agencies to help them protect other IT processes, such as the voter list and result calculation process. The Cybersecurity Agency and the criminal police proved to be particularly receptive. Since then, the EMB has found that even without the official designation of 'critical infrastructure', making the necessary funds available and generating institutional willingness can lead to productive results.

In countries with an independent electoral management model where both the actual and the perceived independence of the EMB is essential, preserving this independence while closely working with security agencies can be challenging (see Box 4.5). In particular, giving other state agencies access to technical election infrastructure for security assessments or requiring security clearances for election workers can become controversial, as this raises the risk of giving the agencies conducting these checks both undue influence over the composition of the election administration and inappropriate access to election data and systems.

Box 4.5. Romania: well-established close cooperation on auditing, but debate about cooperation with intelligence services

Romania's Permanent Election Authority benefits from well-established and comprehensive cooperation with other state agencies and the private sector. For instance, it cooperated closely with the Computer Emergency Response Team for security audits, and with institutions under the Defence Department that provide secure telecommunication and server infrastructure. The Romanian Intelligence Agency is responsible for ensuring the cybersecurity of all state infrastructure, including for elections. Yet given the agency's past abuses of power, its cooperation with other state authorities is controversial.

If agencies have limited mandates and jurisdictions, this can also prevent them from fostering closer cooperation. When resources are limited or the risk of political fallout is high, the agencies not directly mandated to be involved in the electoral process may be especially reluctant to prioritize work on electoral cybersecurity.

4.2.2. Horizontal and vertical approaches

Initiating interagency collaboration and overcoming related obstacles can benefit from both horizontal and vertical initiatives.

Box 4.6. Denmark: thinking big, but starting small—informal collaboration as a starting point

Interagency collaboration in Denmark benefited in two ways at its inception: the absence of strong media pressure and a recent budgetary increase allowed it to commence in a trusting atmosphere. Since then, the cross-agency and partly informal nature of collaboration that was subsequently chosen has proven effective. Command chains have been kept short and there has been a high degree of initiative at the operational level. This has allowed for the fast bottom-up presentation of information to the right decision-makers. Having key personnel meet on an ad hoc basis when needed, instead of through formalized protocols or newly established agencies, has ensured continued ownership and a strong willingness to collaborate.

Horizontal approaches involve agencies instigating cooperation on their own initiative, which can lead to lightweight, efficient and pragmatic solutions. Agencies, often EMBs, set up the initial interaction based on specific needs, exchange contact details, convene meetings, facilitate overall trust building and attempt to bridge institutional gaps. Depending on the country context, informal cooperation may jeopardize transparency and have an adverse impact on the perceived independence of the EMB.

Vertical approaches are based on high-level decisions and shaped in legal frameworks and policies. They can solidify existing collaboration and enable interagency collaboration where less formal cooperation reaches its limits—for example if potential partner organizations do not prioritize joining forces or have the mandate to do so. An official whole-of-government backing through cybersecurity policies and designating elections as critical infrastructure can make required additional resources available, and allow minimum standards to be set in highly decentralized election administrations. A downside of this approach may be concerns about and resistance to 'federal overreach' in highly decentralized systems, such as in the USA.

Whether a horizontal, vertical or a combined approach is preferable depends on various factors, including the size of the country, the nature of existing personal and professional relations, the level of trust between the agencies involved, perceptions of the EMB's independence, and the extent to which the regulatory framework supports or prevents collaboration.

Box 4.7. United Kingdom: building collaboration in unique contexts

Establishing interagency collaboration often does not start in a vacuum. In the UK, the Electoral Commission collaborates with three agencies that existed before cyberthreats in elections emerged:

1. Information Commissioner's Office—the UK's main data protection agency;
2. National Cybersecurity Centre—provides advice and support for the public and private sectors on how to avoid computer security threats (one of the first of its kind in the world); and
3. Constitution Group in the Cabinet Office—has overall responsibility for policy, legislation and funding for UK-wide elections and other polls.

Collaboration in this uniquely chequered environment does not follow international blueprints but grows organically and strengthens with every election.

Few of the case study countries have officially designated elections as critical infrastructure; the meaning and availability of this designation also varies greatly. Finland, for example, reserved this designation for military contexts. Georgia declared that elections are considered critical infrastructure and required the EMB to significantly upgrade its cyberdefences, but did not allocate additional funds or support (see Box 4.8). In the United States, however, critical infrastructure designation was a decisive factor that facilitated the establishment of closer cooperation among the Department of Homeland Security, local election administrators and the Election Assistance Commission because it allowed Homeland Security to provide support to election administrators. In several countries where elections are not officially designated as critical infrastructure, such as Romania, the involved actors still treat them as such. Other countries, including Australia, are considering classifying elections as national critical infrastructure.

Box 4.8. Georgia: critical infrastructure designation and ISO standards

Georgia has classified elections as critical infrastructure, which requires the Georgian Central Election Commission and other agencies to implement its information security management system by considering ISO 27001 requirements, which entails the establishment of comprehensive control mechanisms. Georgia’s Computer Emergency Response Team collaborated closely with the election commission and supported the CEC in implementing its information security management; the team is also available to respond to election-related cyber emergencies.

5. Conclusions and recommendations

1. *Electoral cybersecurity is a long-term commitment that requires implementation throughout the entire electoral cycle.*
   The technologies used in elections potentially change with each electoral cycle, and so do adversaries and their tools. Comprehensive electoral cybersecurity therefore requires continuous commitment and resources.
2. *Even countries that use only limited technology in elections face cyber-risks to electoral integrity that require serious consideration.*
   Until recently, the debate on electoral cybersecurity was mostly about electronic voting; countries with paper-based electoral processes considered themselves largely free of the risk of cyberattacks. There is now widespread recognition that virtually all electoral processes involve technology to some degree, including voter, party and candidate registration, result processing and result publication. Each of these processes can become a target unless it is properly assessed for vulnerabilities and secured.
3. *Interagency collaboration is a key element of improving cyber-resilience in elections.* Electoral cybersecurity threats transcend institutional mandates. Tackling them often requires resources, information, situational awareness and expertise from multiple agencies. EMBs and other authorities working on elections should therefore consider the various models for interagency collaboration on cybersecurity in elections such as those described in this publication.
4. *Managing public perceptions of cyberthreats to an electoral process is as important as defending against actual threats.* Electoral integrity is entirely conditional on public trust and support. Coordinated external communication is therefore integral to countering any disinformation about the electoral process in order to adequately prepare the public for a

potential cyber-related incident and to provide a consistent response if an incident occurs. This publication offers examples of successful models to manage that communication.

5. *Interagency collaboration should be transparent and clearly defined.* In order to safeguard the actual and perceived independence of the EMB, interagency collaboration should be publicly explained. It should clearly define where the involvement of non-traditional agencies, such as the security services, begins and ends. This may require legal regulation stipulating the scope and boundaries of collaboration.

6. *International collaboration is needed.* Cybersecurity in elections is too complex and fast changing to tackle only at the national level. Countries therefore need to invest in bilateral and international knowledge and information exchange. They should do so both regionally and between regions/continents. This publication has shown that different regions are currently moving at a similar speed in the field of cybersecurity. Their variety of experiences, however, offers important potential for cross-fertilization.

7. *Interagency collaboration should go beyond government agencies.* The private sector, political parties, academia, civil society and the media can all play an important role in improving electoral cybersecurity and its public perception. Conversely, actors with an interest or stake in the subject that feel they have no channel to convey their concerns may create additional reputational challenges by leaking information, and possibly exaggerating claims of vulnerabilities. Government agencies should therefore cast their net wide and collaborate with a broad range of non-governmental stakeholders.

8. *Political parties should be made aware of the possibly devastating effects of cyberattacks.* Electoral candidates and (particularly small and less resourced) parties are arguably the weakest link in electoral cybersecurity. In some countries, state agencies can provide basic cybersecurity support and advice. At the very least, parties should be informed of their responsibility to protect their infrastructure and government agencies' limited ability to mitigate the consequences of cyberattacks against parties and their campaigns.

9. *Where spontaneous interagency collaboration is absent, policymakers should consider critical infrastructure designation or other vertical approaches.* Some countries have successfully organized interagency cooperation on a largely informal, horizontal basis on the initiative of one or more of the concerned institutions. Especially (but not limited to) cases in which organic interagency collaboration is absent or has a limited impact, more formal

top-down, vertical approaches may be needed to overcome institutional, cultural or administrative barriers to collaboration, to make funding available and to create the required transparency. Recognizing elections as critical infrastructure is one such vertical approach.

10. *Election observers should assess interagency collaboration.* Observing cybersecurity in elections should include assessing the level and effectiveness of interagency collaboration, including the involved actors, their responsibilities and the measures taken to protect the independence of the election administration.

Annex A: Case studies

A series of case study interviews with EMBs and security agencies from around the world were conducted for this publication. Some of these interviews are reflected in the following country case studies. Other interviews were used to provide additional background information and details.

The interviews were structured by the following themes:

- overview of institution and use of ICTs;
- definition of cyber-risks in elections;
- overview of cyber-risks for election-related systems and processes;
- actors involved in protecting elections against cyberattacks; and
- coordinated cooperation between the relevant actors.

Australia

Structure of EMB

The Australian Electoral Commission (AEC) is responsible for conducting federal elections and referendums and maintaining the Australian Commonwealth electoral roll. Australia has 151 electoral divisions, each of which is represented by a member of the House of Representatives. Divisional offices manage the electoral roll, carry out public awareness activities and administer elections.

Use of ICTs

The AEC has a history of effectively implementing legislative change that requires the use of technology, while maintaining the integrity of the electoral system. It trialled electronic voting for certain groups, including blind and low-vision voters, in the 2007 federal election. This evolved into the current method of telephone voting for these groups.

Currently, the AEC uses various IT systems, ranging from legacy, 20-year-old mainframes to modern cloud-based services. It is responsible for:

- a highly scalable website (from 20 hits between elections to 20 million on election day);
- ballot scanners operated by third-party providers at a counting centre in each state to count the complex preferential ballots;
- a data transmission and tabulation system;
- a voter registration system (hosted by a third-party provider) used to create voter rolls and share voter data with political parties; and
- electronic certified lists in selected locations to find and mark voters off the electoral roll.

Risks

A priority for the AEC is to protect its IT systems—particularly those related to counting votes and transmitting data—and the overall electoral process from integrity challenges. Manual procedures, including a paper count, are always possible and available as a backup plan for a worst-case scenario.

Interagency collaboration

The Australian Government places a high priority on its cybersecurity policy. It provides standard policies and a security manual for protecting the confidentiality, integrity and availability of government data and IT systems in its Protective Security Policy Framework (Australian Government Attorney-General's Department n.d.).

This high standard is not specific to elections; it covers information security in digital and hard copy format as well as physical and personal security. Applying this standard, the AEC treats cyber-risks in the same way as other government entities. Therefore it has a dedicated IT security advisor as part of its Information Security and Governance unit.

Following increasing global concerns, Australia established an Electoral Integrity Task Force in May 2018 to shore up its processes for upcoming by-elections and to inform future federal elections. The task force brings together a range of agencies—the AEC, state and territorial EMBs, the Department of Home Affairs, the Australian Cybersecurity Centre, the Department of

Communications and security agencies. It has assessed vulnerabilities related to elections and electoral processes. The task force seeks to:

- develop a shared understanding of vulnerabilities and how they evolve between elections;
- conduct risk assessments and make related suggestions;
- clarify the role, coordination and leadership between participating agencies;
- advise the AEC and state and territorial EMBs on risk mitigation;
- coordinate the monitoring of social media; and
- develop a joint communications strategy.

Additionally, the Council of Australian Governments has asked that cyber-related 'health' checks are conducted on all Australian electoral commissions. The Joint Standing Committee on Electoral Matters of the Australian Parliament raised the classification of Australia's electoral systems as national critical infrastructure as an important matter for inquiry (Parliament of the Commonwealth of Australia 2019).

The AEC also maintains ongoing communications with social media companies such as Facebook, Twitter and Google to inform management of electoral messaging.

Austria

Structure of EMB

In Austria, elections are managed in a mixed system: an independent Federal Electoral Board (Commission) works with the Federal Ministry of Interior. The different levels of election administration include the federal electoral board, provincial electoral boards, district electoral boards, municipality electoral boards and a special electoral board. Local administrations are responsible for all election operations.

Use of ICTs

The voting process is paper based with manual counts and paper reports. As soon as the polling station is closed the preliminary reports are transmitted via phone, email or text message. These preliminary data are stored on a Ministry of Interior server. These data are not legally binding, but need to be protected from disclosure before voting ends at the last polling station. The digital result figures are compared with provincial reports and the preliminary final results are published on the Internet and announced by the minister. All software is constantly improved and modernized, and the system is tested before every election.

A new centralized electronic voter register was launched in 2018. It facilitates improved data quality and online participation and signing of public initiatives. Municipalities are still responsible for maintaining the local voter registers, but all data are stored on a centralized platform. The added convenience of online participation led to increased interest and unprecedented demand for signing public initiatives.

Risks

The electronic transmission of results consists of ad hoc reports that are not legally binding. The Constitutional Court ruled that only paper minutes are legally relevant for determining the final result. However, even problems with preliminary results may raise doubts: the results publication website led to some discussion when glitches made test data publicly available before election day.

A few days after its launch, the online public initiative system became inaccessible for many users. While the problem was fixed quickly, it triggered a parliamentary inquiry, which established that there were no external (cyber) threats of attacks. It was rather the unexpectedly high interest and load on this new online system that led to very slow response times, but never a full collapse of the system.

Interagency collaboration

Interagency collaboration takes place via Austria's national election network, which was constituted in November 2018. The network covers agencies with mandates related to elections (through the Ministry of Interior, Federal Electoral Board and Foreign Ministry); cybersecurity and network security (through the Federal Chancellery and Ministry of Interior); cyber defence (through the Ministry of Defence); media law, election campaigning and political parties (through the Federal Chancellery); registers and cybercrime (through the Ministry of Interior); online services and digital issues (through the Ministry for Digital Matters); data protection and criminal law (through the Ministry for Constitution, Reform and Justice); and European law and institutional issues (through the Foreign Ministry). The Ministry of Interior serves as the network's national point of contact for the EU.

Bulgaria

Structure of EMB

Elections in Bulgaria are administered by a three-level structure of EMBs: the Central Election Commission (CEC), 31 district election commissions and approximately 12,000 precinct election commissions.

Use of ICTs

Voter lists are extracted from the national population register maintained by the Civil Registration and Administration Services Department of the Ministry of Regional Development and Public Works.

The CEC creates and maintains websites and various registers, and maintains the email system used by the various levels of election administration as well as a system for submitting electronic applications for out-of-country voting. It also enables electronic data exchange for voters and candidates between Bulgaria and other EU member states. It further operates an electronic system for approving pre-printed samples of paper ballots, for electronic results processing and transmission for out-of-country voting.

The election law provides for paper and machine voting. During the 2016 presidential election, machine voting was conducted for the first time at 500 polling stations and the results were official. An experimental machine vote count was also conducted. A pilot of remote electronic (Internet) voting was initiated on 1 January 2018 under the responsibility of the CEC. Preliminary voter lists are required to be posted for public scrutiny at polling stations and on municipality websites at least 40 days before an election. Lastly, the National Audit Office makes campaign-related bank transactions publicly available on its website.

Risks

Following an inventory check of election-related ICT, the CEC adopted a cyber-risk management methodology to identify the possible impact of the risk on the election process, the probability of such risks and remediation measures. This information is updated immediately before an election. The main technical risks covered in the methodology include:

- DDoS—in 2013 and 2015 the commission’s public infrastructure was attacked on an unprecedented scale;
- leaks of voters’/candidates’ personal data (potential threat);
- insufficient competence of election commissions at various levels;
- change of data and content by users with administrative access, by mistake or deliberate;
- fake news (potential threat); and
- information security breach of publicly available resources through attacks involving content change/substitution, including hacking individual machines, attacks leading to equipment malfunctioning, and manipulation

of data during transfer and result processing as potential threats, especially after the introduction of remote e-voting and machine voting.

Interagency collaboration

To protect the election process, the CEC collaborates with a wide range of partners in public administration and technology companies. Bulgaria's e-government and information security operations are contracted to the State e-Government Agency and resources of the Ministry of Interior, the State Agency for National Security and other bodies.

The main technological partner of the CEC is the state-owned company Information Services JSC. JSC experts are in charge of the CEC's critical infrastructure and the development and implementation of computer processing of the results and online attendance when elections are held.

The CEC is responsible for coordinating between all relevant actors, including during an incident. At the national level, an interservice group is chaired by the deputy prime minister, which coordinates and plans the activities before, during and after election day.

Before each election, the public prosecutor general and the minister of interior set up joint headquarters (teams) for operational interaction in the fight against election-related (including cyber) crimes. These teams are operational during the entire pre-election campaign and on election day.

The CEC and its technological partner are continuously improving the cyberprotection methods and technologies. ICT centres for processing election results data are physically independent environments, which prevents external interference during processing operations. The public systems are backed up several times: they are equipped with modern cyberprotection systems and monitored 24/7 by information security experts. The organization's measures for preventing cyberattacks cover the parties directly participating in an election and other relevant parties such as national Internet providers and telecommunication operators, transmission system operators, etc.

A large-scale public information campaign is organized during in the run-up to elections. Regular briefings are conducted, and close cooperation is established with the media in effort to prevent fake news campaigns.

Canada

Structure of EMB

Headed by the chief electoral officer of Canada, Elections Canada is an independent, non-partisan parliamentary agency responsible for administering the Canada Elections Act. The agency's mandate is to:

- be prepared at all times to conduct a federal general election, by-election or referendum;
- administer the political financing provisions of the Canada Elections Act;
- monitor compliance with electoral legislation;
- conduct public information campaigns on voter registration, voting and becoming a candidate;
- conduct education programmes for students on the electoral process;
- provide support to the independent commissions in charge of adjusting the boundaries of federal electoral districts following each decennial census;
- carry out studies on alternative voting methods and, with the approval of parliamentarians, test alternative voting processes for future use during electoral events; and
- provide assistance and cooperation in electoral matters to electoral agencies in other countries or to international organizations.

Use of ICTs

For federal elections, Canada relies on paper ballots that are hand marked by voters and hand counted by officials in some 25,000 different polling stations across the country. This process is observed by scrutineers from each of the major political parties. The election administration is highly decentralized and paper based so documents can be verified after each election. Electronic voting systems are also used. Elections Canada uses new technology to:

- manage electronic networks and intranets at headquarters and in the field to enable communications;
- maintain and improve applications supporting the National Register of Electors and the Electoral Geography Database, as well as several other

tools that support real-time monitoring of (and reporting on) electoral events;

- develop and expand the agency's social media presence;
- create customized applications that support key services, such as the Voter Information Service, real-time broadcasting of election results and online reporting for political entities;
- develop and support customized applications that enable political parties, electoral district associations, candidates, nomination contestants and leadership contestants to complete and submit the financial returns required by the Canada Elections Act; and
- maintain an Online Voter Registration Service, launched in 2012, which offers an alternative way for citizens to check and update their registration status.

Risks

At the federal level, errors in result transmission or attacks against result publication websites may happen, but the results are always verifiable through the paper trail and not even the most sophisticated cyberattack could tamper with them. Local elections are more exposed to cyberthreats, since more technology such as ballot scanners, tabulators and online voting systems is used.

Canada is not immune to attacks designed to suppress the number of people who vote or manipulate how they vote. So far, the only documented attack was the 2011 Robocall scandal, in which thousands of voters in almost 250 ridings across the country reported receiving automated phone messages falsely telling them that their polling station had been changed. Elections Canada's investigations attributed these calls to domestic political actors.

The Canadian Government has tasked the Canadian Communications Security Establishment (CSE) with assessing the cyberthreats to the country's democratic process (CSE 2017) and advising parties on best practices to protect themselves from cyberthreats and to safeguard their databases of personal voter information.

The CSE details three key cyberthreats:

- registering voters: attacks against systems determining who is eligible to vote;
- voting: attacks against systems for receiving, counting and recording the votes; and

- disseminating results: attacks against systems for informing the public of the election results.

The CSE assessment pointed to mostly unsophisticated and low-level attacks in past elections, and highlighted political parties, individual politicians and the media as being the most vulnerable. It expects more (and more sophisticated) attacks in future elections. The assessment concluded that multiple groups will very likely deploy cyber-related capabilities in an attempt to influence the democratic process during the 2019 federal election. This prompted Elections Canada to enhance its cybersecurity posture by improving the security design of its IT network and procuring a new data-hosting service that will offer a range of additional protections, all in consultation with the CSE.

Interagency collaboration

The minister of democratic institutions is responsible for leading the government's efforts to defend the democratic process from cyberthreats, together with the CSE, the Canadian Security Intelligence Service and Public Safety Canada, among others.

In June 2018, the Government of Canada announced the creation of the Canadian Centre for Cybersecurity, which aims to offer a unified approach to cybersecurity and enable faster, better-coordinated and more focused government responses to cyberthreats (which may or may not be election related). Elections Canada works with these security partners to stay up to date on the threat environment. Additionally, the Election Integrity Office, which was established following the 2011 Robocall incident, assesses domestic and international cyberthreats, and aims to prevent them.

Elections Canada coordinates with other government organizations that have mandates related to election security: the commissioner of Canada Elections, the Canadian Centre for Cybersecurity, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, Public Safety Canada and Canada's national security advisor.

The delivery of trusted/secure elections is a joint undertaking involving Elections Canada, security agencies, political participants, the media, private industry and civil society. The efforts span four complementary layers of assurance and collaboration:

1. National security and emergency management, which entails defending Canada against a range of security threats/events including foreign interference and intrusion. The key initiatives are:
    - briefings to political parties and federal/provincial elections officials on threats to electoral processes in Canada;
    - meetings with foreign security and intelligence partners to discuss their efforts and experience;
    - establishing relationships with social media companies;
    - intelligence assessments including the CSE's 2017 report, *Cyberthreats to Canada's Democratic Process*; and
    - various planning and simulation exercises.
2. Democratic institutions, which involves building the resilience of the country's democratic institutions in the context of emerging threats to ensure whole-of-government coordinated action. The key initiative is the passage of the Elections Modernization Act (Bill C-76) in 2018. The bill includes measures that aim to make the electoral process more secure, including by:
    - strengthening the third-parties' regime;
    - adding prohibitions related to the use of foreign funds;
    - giving additional powers to the commissioner of Canada Elections;
    - expanding existing provisions against certain types of online impersonation and false statements; and
    - requiring social media platforms to publish and preserve archives of election and partisan ads.
3. Electoral security, which entails joint efforts to ensure the security of the electoral process. EMB independence is positioned within joint activities and key initiatives:
    - Joint Steering Committee (EMB and lead security agencies)—meets monthly;

   - mandates clarified;
   - interagency collaboration/mutual support instituted;
   - protection of electoral infrastructure strengthened; and
   - outreach to political parties/social media ongoing.

   Planned initiatives:

   - finalization/testing of Incident Management Plan;
   - conduct of various planning and training exercises;
   - finalization of communications strategy; and
   - reinforcement of trusted sources of information.

4. EMB security, which consists of joint work with security partners to strengthen EMB infrastructure and security posture. Key initiatives include:

   - Electoral Integrity and Disinformation team in place;
   - enhanced systems' security and systems' monitoring;
   - launch of security awareness, including field operations;
   - security governance and plan improved;
   - collection/sharing EMB best practices;
   - meetings with political parties; and
   - engaged social media platforms and establishing communication channels to quickly respond to incidents.

   Planned initiatives:

   - continue to establish Elections Canada as a trusted source of information on when, where and how to register and vote;
   - planning/training exercises completed, including election simulation; and
   - social media monitoring.

The overall target is to:

- keep voting simple and convenient and to make basic cyberhygiene accessible to all;
- sustain discussion with political parties and civil society to recognize the political economy of cybersecurity, avoid politicizing electoral security, and manage public and political expectations; and
- facilitate communications through a trusted voice and public spokespersons, dealing with the changing media environment and ensuring coherent and seamless support to citizens.

In early 2019 the Government of Canada unveiled its plan to fight disinformation and foreign interference in a multi-pronged approach that involves the Ministry of Democracy Institutions, Defence and Public Safety, and Emergency Preparedness and builds on four pillars: (a) enhancing citizen preparedness by providing information to the public; (b) improving organizational readiness through improved coordination; (c) combatting foreign interference through security agencies; and (d) expecting social media platforms to help safeguard elections.

Under the Critical Election Incident Protocol, five senior public servants decide when an incident is serious enough to warrant informing the public during the official campaign period. Their decision will be based on information provided by the national security agencies.

Denmark

Structure of EMB

In Denmark, elections are managed by three levels of administration: the Election Section (ES) of the Ministry of Economic Affairs and the Interior (MoEAI), 92 district election committees and some 1,400 polling district election committees. The ES is a permanent body that is responsible for organizing elections. Some ES staff are appointed by the MoEAI to a separate entity, the election board, that performs specific tasks such as registering non-parliamentary political parties that want to contest the elections and maintaining a list of party names, as well as deciding on the eligibility of voters who have resided abroad for more than four years. Staff of the Danish Civil Registration System extract voter registers from the national civil registration system, which contains basic personal information on all residents who have a civil registration number. The MoEAI is responsible for this register.

Subject to a maximum term of four years, Denmark has no fixed date for national parliamentary elections. The prime minister calls an election, which is generally held three weeks later. Party registration in practice needs to be finalized before the election is called.

The MoEAI has responsibility for the election process itself. The wider election integrity agenda—which includes illegal social media activities, cybersecurity and cooperation with political parties—is the responsibility of the Ministries of Justice and Defence.

Use of ICTs

All ballots are hand counted on election night, and a full manual central recount is conducted the next day. District-level vote counts are entered into the election management system (created by a private vendor) and then transferred to Statistics Denmark. For further safeguards, all district-level vote counts are phoned in to Statistics Denmark on election night. The EMB has a fully functional redundant seat allocation calculation. A vote share deviation indicator is also used as a statistical model outlining the probability of the truthfulness of any deviations. It indicates where to look for possible manipulation and errors.

The ES works with three bodies that utilize IT systems:

- the National Registry, which compiles the voter lists;
- private vendors that provide elections technology; and
- Statistics Denmark, which is responsible for collecting the results.

Each of these bodies has its own cybersecurity responsibility; however, if there are any problems the public will look to the ES for a response.

Risks

The decentralized structure of election administration and the largely paper-based process are seen as strengths that make influencing an entire election difficult. One challenge is that local administrations bear considerable responsibility for securing the logistical aspects of elections, including the procurement of systems, but do not always have the necessary capacity or ability to collaborate, for example when assessing their risks. If a threat occurs at the municipal level, the minister will be held accountable by the general public, even if he or she is not responsible. While there is a central manual for conducting elections in local administrations, there are no centralized cybersecurity instructions or guidelines. In 2018, the ES started sending out a letter to warn each municipality about cybersecurity threats.

Although it is hard to disturb elections due to their decentralized and offline nature, a primary concern is the (unfounded) loss of voter trust in the electoral process. Public perceptions are therefore the primary concern, and voter information about how elections work and are secured is important. This information is communicated via both traditional media and social media and helps to kill any rumours that may arise.

The most significant technology-related risks are the defacing of public websites of election-related agencies and major hacks against the providers of key infrastructure including the civil registry and the election management system.

Interagency collaboration

The Danish EMB has no budgetary control over elections; it is only responsible for the legal framework. The municipalities allocate their own budgets and decide about their technology and vendor contracts.

In recent years it has become apparent that there is a need to increase resilience against cyberthreats and to communicate this resilience to the public. The cybersecurity strategy has three aims: (a) to identify; (b) to detect; and (c) to manage and prevent cyberattacks and breakdowns.

On the initiative of the ES, a new inter-ministerial task force was created in 2016 that is coordinated by the Ministry of Justice and includes the Ministry of Culture, Ministry of Defence, the Internal Security Service, the Ministry of Foreign Affairs, and the MoEAI (which participates as the election authority) as well as local administrations. The Ministry of Culture plays an auxiliary role as it is responsible for media regulation.

The fact that the initiative came from within instead of in response to media or political pressure has helped to ensure strong ownership by (and a willingness to collaborate between) the agencies involved. They also have sufficient budget to cover the extra costs. The cooperation is largely informal; meetings are conducted as needed. The task force is deliberately not much more than a phone list including the right decision-makers (sufficiently senior to make decisions, sufficiently working level to know what is going on) and a non-formalized division of responsibilities. This is based on the belief that there should not be a separate system for crises, since systems and institutions should continue to work as they are.

The main purpose of the meetings is to establish the boundaries of responsibility between the agencies, and to exchange information and establish points of contact well before any crisis erupts. Thinking big, but starting small, is seen as a success factor of the task force. The task force has increased awareness among the responsible agencies about responsibilities in this area, and the relevant institutions have showed a great willingness to cooperate. In September 2018, three Danish ministries published a national election action plan against foreign influence on elections and democracy.

Estonia

Structure of EMB

In Estonia, elections are overseen by the seven-member Estonian National Election Committee. The State Electoral Office is the country's top-level EMB. It is institutionally independent but falls under the Chancellery of the Parliament. It conducts elections, and organizes and ascertains the results of Internet voting. It also supervises the activities of election managers and is responsible for the development and management of the technical solutions necessary to organize elections.

Use of ICTs

The State Electoral Office uses a range of election technologies:

- Internet Voting System—operational since 2005, with about one-third of votes cast electronically from 116 countries.
- Election Information System—operational since 1998 as an electronic tool for managing electoral preparations and processing electoral actors, candidates, statistics and results. However, the official results are still the ones from the paper protocols.
- Electoral Results Webpage—publishes the results and statistics from the Election Information System.
- Voters' Register—voters have been drawn from the centralized state population register and maintained by the Ministry of Interior since 2000. An Electronic Voters' Roll (which will allow all polling stations to connect to a single information system) is planned from 2021. The system will draw data from the voter register, but will be the responsibility of the EMB.

Election technologies are part of a broad range of Estonian e-government applications based on public and private sector (energy, telecom, banking) systems. All Estonian citizens carry an electronic ID card to access and use these systems.

While election technologies are the responsibility of the EMB, it is not responsible for electoral campaigns, including social media. However, any illegal social media activities are immediately referred to the police.

Risks

Since the large-scale cyberattacks on Estonia's online and e-government infrastructure in 2007, no more major attacks have occurred. However, there have been minor incidents including the creation of fake versions of the Internet voting website and the EMB's website by political activists. For such incidents close cooperation with the police has ensured a swift reaction.

A main problem in Estonia is not actually hacking or breaching the system, but claiming to be able to hack or breach (any) e-enabled system and therefore undermining trust in elections. Public relations and efficient communication about election technologies are as important as countering actual ICT risks. Countering this threat requires three elements:

- a rigid security system;
- communication of the protection and security measures in place; and
- a fast adjudication process that evaluates the validity of complaints within days (not years).

Quick responses during incidents are critical to maintaining public trust. There is constant collaboration with the police, which removes online disinformation as soon as possible. Estonia's Supreme Court adjudicates complaints within seven days from their filing.

A first comprehensive cyber-risk assessment in 2017 (Past 2017) indicated that political parties and candidates are primary targets for cyberattacks. While the cybersecurity of parties and candidates is outside the EMB's jurisdiction, it has a broader mandate to protect the legitimacy of the election.

In addition, the risk assessment identified three key risk areas:

- all technical systems used in the electoral process;
- risks related to management and cooperation, clear designation of responsibilities; and
- hybrid risks related to information warfare, including on social media, which require a clear communication strategy.

The risk assessment indicated that risk levels rise with the level of election—from low exposure for local elections, to high levels of exposure for national and European elections.

Interagency collaboration

The Estonian EMB views the integrity of elections as the responsibility of the whole government. Cooperation to secure election technology systems includes both the public and private sector: the State Electoral Office together with the National Electoral Committee, the Republic of Estonia Information System Authority, the Response Department of the Estonian Information System

Authority, the Cybersecurity Management Team (CERT Estonia), Cybernetica, and Trust Service Provider (SK ID Solutions). An important security measure is the building of digital hygiene and electronic ID awareness, through which all citizens are encouraged to protect their personal devices and electronic identity.

In Estonia, interagency collaboration takes place through multiple ad hoc task forces and working groups. Splitting collaboration into task forces allows groups to remain small, focused and effective. Task forces work based on personal, professional contacts while working groups are usually conducted between designated representatives of various organizations. Before each election, a number of special groups are formed to tackle specific topics and areas of interest and need. The number and setup of these groups is flexible, based on current events and can be altered if needed. Examples of such groups include:

- The general weekly ICT Working Group is responsible for technologies ranging from information systems, websites to hosting services, etc. The group consists of the EMB, State Information System Authority (SISA) and other relevant authorities on a topic-by-topic basis.
- The Public Relations Weekly Working Group focuses on a clear and unified message about the electoral process and monitoring of messaging around the electoral process, the determination of trigger levels when messages require a response and clarity on how to respond. The group consists of the EMB, the Ministry of Foreign Affairs, the Ministry of Interior, the Ministry of Economics and Communications, the Government Office and SISA.
- The Registries, Voter's Card and Voting Rolls Working Group is responsible for everything related to voter registration and voter lists. The group consists of the EMB, the Ministry of Interior, Ministry of Interior IT Centre and, on some topics, SISA.
- The Campaign Restrictions Working Group discusses the enforcement of limitations on campaign spending. The group consists of the EMB, Police and Border Guard Board.
- The Voting Abroad Task Force is responsible for the organization and administration of voting from abroad. The group consists of the EMB, Ministry of Interior and Ministry of Foreign Affairs.
- The Internet Voting Task Force is responsible for the organization and administration of Internet voting. It consists of the EMB, SISA, the system developer (Cybernetica), helpline and customer support provider (a third-party contractor), and an independent auditor.

Most task forces have developed joint response scenarios. They communicate to the outside world through one dedicated channel, which is usually the EMB's communication person. Important for the efficient operation of these groups is that they convene meetings between equals of their respective organizations: senior staff meet with senior staff, IT experts meet with IT experts, etc.

The EMB also cooperates with SISA and offers cyberhygiene trainings customized to the needs of political candidates. This includes instructions on using social media, securing accounts, recognizing and preventing phishing attacks, etc. Similar trainings are offered to political parties, including a security review of all their electronic channels and online presence. These trainings and services are not mandatory, but political stakeholders find them very useful. Additional bilateral cooperation takes place with Denmark, Finland, Latvia and Sweden, and Estonia contributes to EU efforts on cybersecurity in elections.

European Union

Election administration mandate

The organization of elections in EU member states falls strictly under member state sovereignty; the EU only has a weak election mandate. However, in the context of increasing threats, fears of the EU overstepping its boundaries have gradually given way to a realization of the need to increase cooperation.

Risks

Previous cyberattacks have received little public attention. As these attacks became part of the mainstream debate, it became clear that there is a need for standards, for increasing cooperation and to address cyberthreats more broadly than the electoral process. There is also a recognition that a breach in any of the 27 member states during the European Parliamentary elections can have an impact on the ability of the European Parliament to convene.

In September 2018, the European Commission presented the package 'Securing free and fair European elections' that contains several documents, including a communication, guidance, recommendation and draft regulation. The goal is to increase cybersecurity, and to regulate (online) political campaigning, online transparency, the fight against disinformation and data protection.

The package builds on the EU's Compendium on Cybersecurity of Election Technology (NIS Cooperation Group 2018); the EU *Code of Practice on Disinformation* (EC 2018d), which sets out self-regulatory practices for online companies; the *Action Plan on Disinformation* (EU 2018c); and a *Recommendation on Election Cooperation Networks, Online Transparency, Protection against*

Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament (EC 2018b).

The EU *Directive on Security of Network and Information Systems* (EU 2016) led to the creation of a coordination group among all member states. The group distinguishes between cyberthreats at the *technical level* and *information operations*, which are often more visible. The coordination group provided a platform for initial cooperation on cybersecurity and elections and the drafting of the compendium.

Interagency collaboration

In its recommendation on election cooperation networks, the European Commission (EC 2018b) recommends that 'each Member State should set up a national election network, involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing rules related to online activities relevant to the electoral context [...] and also:

- Facilitate the swift, secured exchange of information on issues capable of affecting the elections to the European Parliament including by jointly identifying threats and gaps, sharing findings and expertise, and liaising on the application and enforcement of relevant rules in the online environment.
- Whenever appropriate, in accordance with national law, consult, and cooperate with the relevant national law enforcement authorities. Where appropriate, cooperation between national law enforcement authorities at European level may be facilitated by Europol.
- Member States should provide the necessary support to the networks referred to in point (1) and ensure that they have the necessary means to allow a rapid and secure sharing of information.
- In order to facilitate the sharing of expertise and best practices among Member States including on threats, gaps and enforcement, each Member State should designate a single point of contact.
- Member States should adopt specific technical measures to ensure the availability, authenticity, confidentiality and integrity of election services relying on network and information systems. To guarantee the smooth running of every phase of the election, Member States should adequately protect networks and systems used for registering voter rolls and candidates; collecting, processing and counting votes; publishing and communicating election results to the wider public.

- European and national political parties, foundations and campaign organisations should implement specific and appropriate measures to prevent cyber incidents and protect themselves against cyberattacks.
- Member States should perform a comprehensive assessment of risks associated with the elections to the European Parliament with a view to identifying potential cyber incidents that could affect the integrity of the electoral process. Member States should put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks, aiming to minimise their impact, and guarantee a swift exchange of information at all relevant levels, from technical to operational and political. In order to do so, Member States should make sure that national authorities with competence for electoral matters have adequate resources, including technical equipment and trained personnel, in order to deal with such incidents.
- Member States should engage with third parties, including media, online platforms and information technology providers, in awareness raising activities aimed at increasing the transparency of elections and building trust in the electoral processes.
- In the event of a cyber-incident involving attacks against information systems that target the electoral process, Member States should consider an appropriate criminal law response on the basis of Directive 2013/40/EU on attacks against information systems. Member States should ensure close cooperation between national competent authorities, cybersecurity authorities and law enforcement authorities.'

In March 2019, the European Election Cooperation Network organized a first tabletop exercise to test the EU's cybersecurity preparedness ahead of the 2019 European Parliament elections. This exercise (EC 2019) allowed participants to:

- 'acquire an overview of the level of resilience (in terms of policies adopted, available capabilities and skills) of election systems across the EU, including the level of awareness among other stakeholders (e.g. political parties, electoral campaign organizations and suppliers of relevant IT equipment);
- enhance cooperation between relevant authorities at the national level (including election authorities and other relevant bodies and agencies, such as cybersecurity authorities, Computer Security Incident Response Teams, the Data Protections Authority, authorities dealing with disinformation, cybercrime units, etc.);

- verify EU member states' capacity to adequately assess the risks related to the cybersecurity of European elections, promptly develop situational awareness and coordinate communication with the public;
- test existing crisis management plans as well as relevant procedures to prevent, detect, manage and respond to cybersecurity attacks and hybrid threats, including disinformation campaigns;
- improve cross-border cooperation and strengthen the link with relevant cooperation groups at the EU level (e.g. Election Cooperation Network, NIS Cooperation Group, Computer Security Incident Response Team Network) in order to improve the capacity to respond in a coordinated manner in the event of cross-border cybersecurity incidents; and
- identify all other potential gaps as well as adequate risk mitigation measures that should be implemented ahead of European Parliament elections.'

Finland

Structure of the EMB

Finland's supreme election authority is the Ministry of Justice (MoJ). Local authorities responsible for elections include 13 electoral district committees and 311 municipal authorities and municipal election committees, as well as election committees in about 2,000 polling stations. Additional election committees are in place in around 500 advance polling stations as well as in institutions such as prisons and hospitals.

A close partner of the MoJ is the Population Registry, from which the election administration obtains the voting registers, and the Ministry of Foreign Affairs, which takes care of the advance voting from abroad. Data protection is a key security concern for all agencies dealing with voter registration.

Use of ICTs

The Finish Government agencies distinguish the technology they use on two levels:

- Low-level systems are generic software applications that are maintained by a joint agency, in cooperation with outsourcing partners.
- High-level systems are specific systems tailored to each agency. Three companies are involved in running the current set of election-related applications.

Finland's Election Data System is the IT system used for most national nationwide elections (except Åland, municipal referendums and Sami's parliamentary elections). The system consists of five subsystems:

- the Base Data System (management of election districts, election authorities and their users, contact information, polling stations);
- the Voting Right Data System (voter register and related systems for update and analysis);
- the Candidate Data System (parties, candidates, candidate list registration);
- the Result Calculation System (vote tabulation and result calculation); and
- the Result Reporting System (official reports on election results and various statistics).

The system is owned by the MoJ; its data are jointly owned by the MoJ and the Population Register Centre, and the Legal Register Centre administers and operates the system. The system is custom developed by five companies. It is web based with different user access levels, and most functions are restricted by date and time. A separate system gives voters access to public information. Work on the system started in 2002; it has been in full use since 2012.

Finland conducted an online voting study in 2017 and decided not to adopt the practice, mainly for security reasons, especially regarding the security of the end user devices and the high costs of a secure system. Only the autonomous region Åland conducts online voting as of 2019 for its small population of 30,000, many of them abroad.

Risks

The most critical processes in the system are:

- the voter lists, due to the sensitive, personal data they contain, directly exported from the population register, combined with the need to make these data available in polling stations as paper copies;
- the result calculation system, used in all voting areas to enter results data; and
- the result publishing system to disseminate the results through separate channels via the MoJ website and media companies.

Cyberthreats against those systems are taken seriously, especially from ideologically motivated attackers who may be very persistent. However, some of the same tools that are used by well-resourced adversaries in advanced persistent threats are also available to bored individuals who may also have the patience and resolution to launch successful attacks. In light of increasing risks, the EMB has received considerable additional funding to set up more secure practices. Safeguards for the system include creating paper records of every critical process that can be verified independently from IT systems.

Interagency collaboration

Beyond the cooperation with the Population Registry on voter registration, election-related technology is the responsibility of six key organizations:

- the MoJ election unit responsible for overall electoral matters;
- the ICT Service Centre that is directly responsible for the Election Information System;
- three private ICT service providers contracted by the MoJ;
- the State IT Agency;
- the State Cybersecurity Agency in an advisory role, which analyses threats; and
- the Central Criminal Police, which is responsible for investigations.

Additional cooperation needs to be established with a newly created agency responsible for the central authentication system and electronic identification for the entire government.

Basic coordination between these agencies has been in place for decades. However, starting in 2016 closer cooperation was initiated by the EMB. As elections are now understood to be sensitive to security threats, the Cybersecurity Agency and police are now more closely involved in this cooperation. Elections and other government systems are not defined as critical infrastructure; this designation is mostly used for military contexts.

Additional cooperation with ministries and academia was initiated in 2017 related to the introduction of postal voting and the debate about introducing online voting. While postal voting and a related new ICT system are being introduced, online voting was not universally adopted due to security concerns.

Interagency collaboration takes place in different formats:

- meetings between agencies on multiple topics including cybersecurity that take place at irregular intervals with various agencies attending as needed;
- a continuously updated risk overview and related mitigation measures, based on threat assessments and intelligence—a specific cyberassessment,

including ongoing international developments, is conducted for each election;

- development of plans to handle crisis events involving all parties, including investigation capacity; and
- exercises and simulated scenarios (mostly tabletop exercises) analysing scenarios step by step, clarifying responsibilities, preparing investigations and handling incidents.

Most of this collaboration is informal, with little published information. Written records of activities are only provided to the minister of justice. The security sector does not necessarily agree that elections are their responsibility. Cultural and language barriers impede collaboration between stakeholders with a government/legal and military background.

Although the EMB maintains contact with social media providers, it does not consider itself responsible for disinformation they disseminate. Nor does the EMB believe the security of political parties' technology is a government responsibility.

For information influencing, including on social media, Finland maintains a cross-government counterinformation system to coordinate its response in cooperation with NGOs and the media. It also hosts the Helsinki European Centre of Excellence for Countering Hybrid Threats. This interagency taskforce is responsible for creating public awareness of hostile information activities, training local election authorities, and informing the media and the public about the resilience aspects of elections, and serves as a network for government agencies conducting traditional and social media monitoring internationally.

For overall public communication, the prime minister's office issued the Central Government Communications Guidelines (Finland Prime Minister's Office 2016) that highlight the importance of interagency collaboration:

> The best buffers against information by influence are efficient cooperation between authorities, a high level of general education, good media literacy and a media committed to good journalistic practice. It is important to respond to manipulative dissemination of misleading information quickly by communicating truthful information. Special care needs to be taken to ensure that correct and reliable information published by public authorities is easy to find.

Georgia

Structure of the EMB

The Central Election Commission (CEC) of Georgia is an independent administrative body; it is free of any influence from other state bodies. The CEC is responsible for the preparation and conduct of referendums, plebiscites, presidential and parliamentary elections, and the elections of local self-government representative bodies (*sakrebulo*) and local self-government executive bodies (mayor/*gamgebeli*). The CEC compiles the voter list data from the MoJ's Public Service Development Agency.

Use of ICTs

The technology used by the CEC includes:

- an Electoral Management System;
- a results processing system to transmit data starting at the district level;
- a public website;
- a searchable voter register for personal data verification; and
- an election results interface.

Vote counting technology is currently being researched.

Risks

In the summer of 2008, Russia waged a short but intensive war against Georgia. Alongside physical attacks, cyberattacks all over the country targeted several government agencies, ministries, media and online forums. This war was the starting point for the following initiatives:

- the establishment of the Data Exchange Agency in 2010, governed by the MoJ with core functions related to e-governance, data exchange and infrastructure and information security;
- The establishment of the Computer Emergency Response Team (cert.gov.ge, CERT) in 2011, operating under the MoJ's Data Exchange Agency, which is responsible for identifying, registering, analysing and responding to incidents affecting government networks and critical infrastructure;
- the 2012 Law on Information Security; and

- the designation of the CEC and elections as critical infrastructure, which requires the CEC to implement its information security management system by considering ISO 27001 requirements.

Georgia has not experienced any more major cyberincidents in elections since 2008.

The CEC's risk management policy is based on three principles—confidentiality, integrity and availability. Most information managed by the CEC is public and therefore information integrity and availability are of the highest priority; websites and online systems face the highest risk levels. Confidential information is largely limited to the personal information provided on voter registers. Voter registers are public and available online; however, personal details can only be accessed by each citizen after presenting her or his personal ID number.

Interagency collaboration

The CEC and its Information Security and IT department are responsible for the security of election-related ICT systems. Georgia's Data Exchange Agency and CERT stand ready to provide emergency assistance in case of cyberincidents. The CEC also receives support and advice from CERT, including on the implementation of security measures that are required as part of the critical infrastructure designation. This includes the establishment of an information security management system.

Meetings between the CEC and CERT are conducted as needed. CERT provides recommendations and information about new developments and areas where security needs to be strengthened and advice on the procurement of new ICT systems.

The CEC also maintains a cooperation agreement with the police, who provide support if an incident occurs. In areas where the CEC lacks sufficient internal resources, including to protect against DDoS attacks, the CEC also works closely with the private sector and Internet service providers. The CEC does not maintain official contacts with social media providers, but may build such contacts in case electoral process-related disinformation is disseminated in the future.

No proactive public outreach in relation to cybersecurity is conducted prior to elections, and the CEC rarely receives questions from stakeholders. However, an incident management policy is in place that defines the roles and responsibilities in case of incidents, including clarification about when public communication and media announcements will be made.

Latvia

Structure of the EMB

Elections in Latvia are run by the Central Election Commission (CEC), which is an independent body responsible for conducting *Saeima* (parliament) elections, European Parliament elections, city council and municipality council elections, as well as national referendums. The commission deploys regional electoral commissions (119 regional polling stations) and municipal electoral commissions (1,100 local polling stations).

The *Saeima* elects the chairperson of the CEC and seven commission members. The Supreme Court, at its plenum, elects one commission member from among the judges. In practice, the chair and vice-chair of the election commission are non-partisan, while its other members are party nominees.

The State Chancellery comprises the prime minister's office and related departments. It prepares Cabinet meetings and coordinates planning of national policies, and has a coordinating and preventative role on cybersecurity. It organizes courses and trainings for the EMB, and state and private media. Trainings focus on preventing, crisis response and communicating with the media.

Use of ICTs

The use of ICTs in Latvian elections is limited: it has no electronic voting and no voter register. Instead, Latvians use their passports to identify themselves at polling stations. Counting takes place at decentralized locations, where ballots are scanned and projected on a big screen so that all those present can scrutinize the process. The results management system is separate from EMB servers and is only deployed during the electoral period. The EMB transmits results electronically, but uses paper backups.

Elections in Latvia are designated as critical infrastructure. In practice this affects the institutions that are involved, the standards that are applied and the mandatory levels of security, and ensures that 24/7 support is offered in the event of a crisis.

Risks

Power or Internet outages are considered risks for which backup plans have been created. Otherwise, the State Chancellery considers unbalanced reporting to be a more significant risk than hacking of election technology.

Latvia has not had any recent cases of fake news affecting elections or direct voter suppression tactics. Rather, it has experienced indirect voter suppression from 20 years of Russian information flows, which the State Chancellery considers as presenting a more negative and less balanced view of Latvian current affairs. For instance, Russian information provides a negative view of NATO, and dedicates disproportionate attention to just two of Latvia's political parties.

Interagency collaboration

Latvia maintains interagency collaboration in a Cybersecurity in Elections working group that includes:

- the Computer Emergency Response Team (CERT);
- the State Security Service;
- the Latvia State Radio and Television Centre, who provide telecommunications security, for instance in protecting against DDoS attacks;
- private companies that develop relevant software; and
- other actors are involved on an ad hoc basis.

These actors collaborate with the EMB but ensure that it maintains its independence. The State Chancellery also created a disinformation task force in July 2018 that has the following roles:

- monitoring information on traditional media and social media, regarding external influencing;
- working with social media, NGOs and political parties; and
- educating the EMB.

The task force seeks to ensure that the Russian narrative does not exert undue influence on the Latvian media or citizens' views. It counters imbalanced information by:

- developing disinformation campaign scenarios (before, during and after elections) and running simulations with media, law enforcement agencies and the CEC to help them decide what to do in case of incidents; and
- training media, law enforcement agencies and the CEC (with input from Google) on how social media work, how to check sources, how to recognize fake news, and how to recognize trolls and bots on social media.

The task force was initiated in the lead-up to the general elections on 6 October 2018. It was established by the prime minister's office in the State Chancellery, which allows the task force to coordinate most effectively with all related departments and security agencies. The task force convenes on an ad hoc basis and when needed.

Mexico

Structure of the EMB

The National Electoral Institute of Mexico (INE) is an autonomous, permanent entity responsible for organizing and overseeing federal elections in Mexico, and for collaborating with local EMBs to jointly conduct local elections. The supreme directive body is the General Council.

The INE's responsibilities and mandate have increased over time and now include electoral training and civic education at the national level, boundary delimitation and voter registration, polling station designation and appointment of poll workers, rules on preliminary results, opinion polls, quick count and electoral materials, and oversight of political parties and electoral campaign financing. The Electoral Court is a separate body responsible for electoral dispute resolution.

Use of ICTs

The INE uses state-of-the-art technologies for its internal systems, including firewalls and cloud services and 35 information systems. It contracts the monitoring of its systems to third-party providers.

Electronic voting is only allowed for Mexicans living abroad, but as of 2018 only 3,000 voters had cast their vote online. The INE is working on implementing increased online voting capabilities for future elections, but there are technical hurdles (e.g. the lack of electronic identification) as well as political obstacles to proceeding.

Risks

DDoS and other hacking attacks have been attempted for many years. Several technologies used by the INE are online and therefore vulnerable to cyberthreats:

- website and online applications;
- polling station status monitoring system; and
- interactions that require the system to be available.

The INE deals with direct disinformation targeted to voters on social media, but has no jurisdiction over problematic messages, such as fake news. To tackle disinformation about the status of polling stations, it has developed a mobile application that enables monitoring teams to visit polling stations on election day, verify any issues, and notify the INE (which in turn notifies social media providers) about messages that need to be taken down. Following an online incident, the INE began collaborating with social media in 1998 and is now in close collaboration with Google's political division and has signed Memoranda of Cooperation with Facebook (El Universal 2018) and Twitter (INE 2018).

The INE also conducts media monitoring from a financial perspective. For example, political parties are not allowed to buy airtime. Accordingly, the INE has made arrangements with Facebook and Twitter to monitor political parties' adherence to the rules. Online campaigns with websites located outside Mexico are beyond the INE's jurisdiction.

Interagency collaboration

Mexico's interagency collaboration on election security has been designed from the top down and has been in place for many years. The INE collaborates with a broad range of actors:

- universities;
- National Security Agency's emergency response team;
- telecom operators, which freeze all system changes during election week;
- electricity providers, to minimize power interruptions; and
- government construction sector, to freeze construction work on election day to prevent disturbances.

Election technology security is overseen at three levels:

- an internal security group of 15 security experts;
- an external security group that checks systems through a private company; and
- universities, which provide a third layer of verification to build confidence in the systems.

Mexico is debating whether to designate elections as critical infrastructure. It has a highly transparent procurement process that may be at risk of revealing sensitive information during tendering processes. There are similar concerns regarding freedom of information requests of sensitive information. Designating elections as critical infrastructure would allow restrictions of transparency in such areas.

Moldova

Structure of the EMB

Moldova's CEC is institutionally independent and autonomous from the executive branch of government. Lower-level EMBs under its jurisdiction are responsible for conducting elections at the sub-national level, with the exception of the Electoral Commission of the Autonomous Territorial Unit of Gagauzia. Moldova has a passive automatic voter registration system. The voter lists are generated from the State Registry of Voters that is connected with the State Register of Population, which is updated daily.

Use of ICTs

The CEC carries out a number of activities using new technologies:

- Tabulation takes place in both paper and electronic form.
- A digital voter register records voters at polling stations, as an additional verification mechanism parallel to a paper voter list.
- The CEC takes its voter list data from the State Registry of Voters, which is managed by CEC representatives.
- The CEC website live streams counting in polling stations.

Risks

The digital voter register is connected to CEC servers through the Internet. There is a risk of a cyberattack on election day, when each locality enters polling station data to the register of voters, which is subsequently transmitted to the CEC. Given the decentralized nature of the system, even a single case where the system is compromised, either through human or technical error or through an actor-driven attack, would affect the credibility of other modules linked to the register, such as the voter lists and candidate lists.

Interagency collaboration

To counter such risks, the CEC formed a joint working group in 2014 with the Information Technology and Cybersecurity Service and the Security and Intelligence Service that discusses possible threats, response scenarios and the division of roles to address threats. These agencies operate under ISO 27001 information security standards, which has helped design procedures to plan and act in various scenarios. On certain issues, agencies such as the Ministry of the Interior and Internet providers are also involved.

The working group convenes only six months before an election, increasing to daily meetings in the week before an election, and has an on-site presence on election day. Since elections usually take place annually, this collaboration has become strong, a sign that interagency collaboration strengthens with more frequent elections. Ongoing discussions revolve around the management of some of the technology hardware; the CEC believes its responsibility for this clashes with its role as electoral administrator.

For some of its communication systems, the CEC relies on the security services. For instance, the Security and Intelligence Service is responsible for announcing any DDoS attacks to the public. Day-to-day cooperation between the CEC and the security agencies happens at the technical/operational level on a daily basis, with senior-level involvement in decision-making as needed.

The CEC does not work with social media providers or engage in communicating cyber-risks to the general public. Nor do the security agencies or the CEC provide support or guidance on cybersecurity at the local level, even if the CEC considers local-level access to the voter register to be a big risk.

The Netherlands

Structure of the EMB

Elections in the Netherlands are highly decentralized, which affects interagency collaboration. The roles of the EMB are divided between the Electoral Commission (*Kiesraad*), the Ministry of the Interior and individual municipalities:

- The country's 355 municipalities are primarily responsible for organizing the vote, such as printing ballots and setting up 9,500 polling stations.
- The Electoral Commission is responsible for preparing candidate lists, aggregating votes at the national level, declaring the national result and advising the government. In the past, it has also made software available to municipalities.
- The Ministry of the Interior holds political responsibility for the implementation of the Electoral Law and creates related policies, rules and regulations. In cases of electoral disruptions, parliament can hold the minister to account.

The Ministry of the Interior fulfils three roles in the area of cybersecurity in elections—through its Directorate for Elections, the General Intelligence and Security Services, and the National Cybersecurity Centre.

Use of ICTs

Technology in the Dutch electoral process includes the following:

- The voter register is extracted by municipalities from the Citizen Register, which is maintained and updated by the tax authorities. Voter lists for polling stations are paper based, but the personal information processed to create voter lists is part of the critical election infrastructure.
- With the abolishment of electronic voting in 2006, the most important remaining ICT system is the software OSV, which is used at the municipal level to aggregate the manually counted polling results, and to calculate election results.
- The tablet-based turnout application (StembureauApp) and ID card scanner.
- Some municipalities have recently introduced privately developed polling results applications to facilitate the tabulation of votes.

Risks

The main risk area for the Electoral Commission is currently the OSV software. In 2017, a Dutch white hat hacker group attempted to demonstrate that OSV is not secure. Even though the commission did not agree with this analysis, the media and political impact led the minister of the interior to abruptly abolish OSV. Municipalities and the Electoral Commission objected.

Public awareness and debate over OSV since then has demonstrated that perceived cybersecurity risks can become almost as disruptive as actual cyberinterference. It also showed that old security principles and software form a major challenge in the face of new cyberthreats. Software updates alone are not enough; procedures and hardware need to be updated as well.

Interagency collaboration

As a result of public awareness and the media fallout regarding IT in elections, the multiple agencies have struggled to define their responsibilities with regard to cybersecurity in elections; the electoral law is largely silent on this issue. In early 2018, an outside agency was appointed to explore the responsibilities of all actors involved, and to map how to help each actor fulfil its responsibility, including by ensuring the necessary knowhow, resources and political backing.

In response to previous media encounters, the Electoral Commission has taken three steps. First, it has prepared ready-made responses in case perceived or real IT weaknesses occur. Second, whenever it adjusts its IT systems, it takes into account potential public criticism in the design process. Lastly, the commission involves external IT experts to advise on potential weaknesses.

Norway

Structure of the EMB

Norway's Ministry of Local Government and Modernization is responsible for the overall organization and conduct of national and local government elections, creating the legal framework and approving pilot schemes. It also serves as an appeal body to hear disputes involving local elections.

The Directorate of Elections provides a centralized computer system that is used for elections, guidance and training for local government authorities, and providing information to the general public. The directorate also produces and distributes election material and provides information on election results.

The election administration is decentralized to EMBs at the county and municipal levels, including 30,000 election staff working on election day who are responsible for the practical conduct of the election from approving party lists to counting the ballots. Decentralization is thought to help protect the electoral process; so far no attacks have occurred.

Use of ICTs

Norway's election administration system (Elektronisk Valgadministrativt) was initially designed for the 2013 elections. It covers the entire electoral process, from candidate registration to election result processing, and includes technology for electronically marking the electoral roll as well as centralized ballot scanning. In 2011 and 2013 an Internet voting system was piloted, but then cancelled due to debates about its security.

Risks

The security of the electronic computer system was challenged in 2017, first on social media and then in the mainstream media. Ten days before election day new regulations were issued that stipulated that all municipalities must manually count the preliminary vote. This requirement will be re-evaluated for upcoming elections.

While the election administration system is well tested and secure, the new regulations were issued to avoid any speculation or uncertainty about the election results as security and trust are vital to the conduct of elections.

Interagency collaboration

For the 2017 parliamentary election, informal cooperation with the MoJ, the Norwegian National Security Authority and the Security Police was established to:

- monitor the electronic administrative system to detect and prevent digital operation;
- observe social media activity;
- conduct election-specific threat assessments;
- provide information to the political parties and central stakeholders; and
- offer advice and information to local election management.

This collaboration is in the process of becoming formalized.

Romania

Structure of the EMB

The Permanent Electoral Authority (PEA) is the permanent EMB of Romania. Three months before an election, temporary electoral bureaus are established, centrally and in up to 3,000 local jurisdictions, depending on the type of election. The Central Electoral Bureau consists of judges, commissioners and party representatives and oversees the election. Local election bureaus are responsible for conducting elections in up to 18,000 polling stations. The electoral bureaus' work ends once the official results have been published.

Voter registers are based on data extracted from the civil registry, which is maintained by the Ministry of Interior; through that, citizens are registered automatically when they turn 18 years old.

Use of ICTs

The main IT system used between elections is the voter register, which is managed and updated regularly by staff from mayors' offices throughout the country. This process provides the basis for updated electoral rolls for the election bureaus to use on election day.

The PEA provides all electoral bureaus with online tools, accessible through a private network, that support electoral tasks such as polling station management, results management, data transmission and online result presentation. Polling stations use an electronic turnout monitoring system based on ID card readers to prevent ineligible and multiple voting. The PEA also operates a results tabulation and seat allocation system, and has a web presence and online data feeds to electoral stakeholders to publish election results.

Technology has played an important role in building trust in elections. The number of complaints about the voter register, voter impersonation and multiple voting has decreased, and has stopped malpractices such as the bussing of voters.

Risks

The main cyber-risks are related to the online voter register and other online assets of the election authority. Cyberprotection measures need to be prepared for the PEA and all electoral bureaus, and protection is based on principle of resilience of all involved bodies.

Protection mechanisms are based on scenario development and analysis and the simulation of responses to various security breaches. The ultimate main security feature and possible fallback option is the mandatory paper trail for the whole process. If an incident occurs, the paper trail contains official information that can be used to investigate any discrepancies in the ICT system.

Online systems have been exposed to many attacks such as DDoS, attempts to deface websites, scamming and structured query language injection. However, none of the attacks was very sophisticated or created significant damage.

A more serious attack vector is disinformation about PEA IT systems. In previous elections the PEA has been faced with media claims that there are shortcomings in the election IT system based on misleadingly interpreted tender documents. This had a negative impact on both the credibility of the IT systems and the PEA as a whole. These incidents showed that disinformation about the electoral process is difficult to manage once it has reached a wide audience.

Interagency collaboration

The PEA does not have a dedicated cybersecurity team. The regular ICT staff is responsible and has support from other agencies. While elections are not officially designated as critical infrastructure, most involved actors treat them as such.

For the voter register, Romania’s CERT conducts a security audit and makes related recommendations every year. After an attack, log files are provided to CERT for analysis. Additionally, a private company provides security audits every two to three months.

In non-election years security audits of the PEA are conducted in cooperation with the Special Telecommunication Service, which has military status and provides secure communication facilities to all state institutions and coordinates related activities. It is also the PEA’s closest collaboration partner on cybersecurity. Ongoing cooperation includes security audits that are conducted whenever election technologies are modified or expanded. The Ministry of Defence provides the EMB with off-site backup server infrastructure located at military installations.

Security measures are increased in election years, which entails collaboration with CyberIT, a unit of the Romanian Intelligence Agency responsible for ensuring the cybersecurity of all state infrastructure. CyberIT also conducts nationwide, interagency scenario-based cyber exercises with a broad range of actors from academia to secret services and the election administration. There is public debate about the cooperation between intelligence services and other state actors, due to the problematic history of the intelligence services in Romania.

Following the media allegations that undermined trust in the PEA's technology, since 2016 the commission has invited political parties to send experts to audit all election technology, including inspecting the source codes for results processing and the calculation of mandates. Party representatives are allowed to run and verify these systems on their own computers and replicate the entire results process themselves. They can also participate in an event shortly before and after each election that demonstrates that the system they verified is in fact the one used by the PEA.

Romania has not experienced large-scale foreign or other disinformation campaigns. Although technical measures have been in place for a long time, old urban myths and rumours still resonate among the population, for example about double voting and deceased voters on the list.

Cyberhygiene training programmes for political parties are being introduced to protect their internal information as well as election-related data provided by the PEA. Any hacks or data leaks from parties may therefore also create the perception of a successful attack on the PEA.

South Africa

Structure of the EMB

The Independent Electoral Commission (IEC) of South Africa is a permanent body created in the country's constitution to manage free and fair elections at the national, provincial and municipal levels of government. Although it is publicly funded and accountable to parliament, the IEC is independent from the government.

IEC provincial offices are responsible for activities in each of the nine provinces. Each provincial office has a provincial electoral officer and support staff. The provincial offices oversee 213 municipal electoral offices and 70 sub-offices, and manage electoral projects, including elections.

The IEC manages the entire elections process, from planning to reporting the results. Social media are outside the IEC's mandate.

Use of ICTs

Voting, vote counting and local vote tallying are conducted manually. A centralized system is used for double-blind result capturing, aggregation and seat allocation as well as auditing of the results. The results are published in real time, with raw and aggregated data available for media and political parties. Scanned images of results slips are also available.

Other uses of technology are related to operational and management support:

- registration of voters, political parties, candidates, including citizen portal and online self-service tools (candidate nomination, registration status, special votes, etc.);
- the IEC's web presence, including the online voter register; and
- administrative back-office and collaboration systems, business intelligence, issue, asset and staff tracking.

ICT security focuses on all levels, including multi-layered network segmentation, security-driven application design and development, user account management and access control on a need-to-know basis, online traffic filtering for malware, continuous security monitoring and timely information sharing about any breaches.

Risks

Protecting these systems against cybersecurity threats is an important part of the daily monitoring of security matters around elections and part of the IEC's obligations and duties 'to develop and promote the development of electoral expertise and technology in all spheres of government'.

The IEC's key security considerations are openness and transparency. It emphasizes making sure that the information it shares is accurate. It detected and stopped hacking attempts in 2011 and 2014 against its website; the former was deemed severe enough to warrant a State Security Agency investigation. The IEC has not experienced a severe cybersecurity breach since then.

Interagency collaboration

The IEC has only limited reliance on other state institutions and only within their constitutional roles, including the police, security, etc. It does rely on private companies to provide specialist services. In South Africa, election security monitoring and readiness assessment occur at multiple levels:

- The IEC appoints independent commercial contractors to conduct security assessments with various levels of access to internal systems to prepare for elections.
- The Auditor General's Office conducts security audits and is provided with all required access.

- The IEC's IT Department and Department for Electoral Matters audit the result system for legal compliance, access control and security.
- The State Security Agency provides the IEC with a threat analysis, highlights areas that need attention (generally not including cybersecurity) and can investigate incidents as needed.
- Cooperation with the police on overall security matters is long established. However, this does not include the cyber domain.

In every election year, the IEC commissions an independent security audit of its entire ICT infrastructure, including external penetration testing through internal security controls and policy implementation, and software patch levels to identify all possible security risks and vulnerabilities. The external auditor provides an assurance report to both management and stakeholders, including remediation guidelines to technical support teams. Additionally, political parties are invited to independently audit the results system, to assure themselves that the system works as intended and prescribed in law.

Political parties asked the IEC for cybersecurity advice, which evolved into monthly Party Liaison Committee meetings (and more frequently in the run-up to elections). Small parties have very few resources and are therefore more exposed to risks and need additional support. However, parties' cybersecurity is outside the mandate of the IEC, which can only encourage security agencies to provide more information to political actors. Overall, the IEC is planning to focus more on a broader, common understanding of emerging cyberthreats among electoral stakeholders.

Sweden

Structure of EMB

The Swedish election administration is highly decentralized. The main central agency, the Swedish Elections Authority (*Valmyndigheten*), has around 20 full-time employees and supports and guides 21 counties, each of which has one or two people working on elections. Below the county level are 291 municipalities. About eight to nine months before election day, the election workforce grows from 1–3 persons to approximately 10 staff per county and municipality for central administration. A large number of extra polling station personnel are also recruited for each election.

The Election Authority's mandate is focused on planning and implementing the electoral process including party registration, provision of electoral materials (establishes electoral rolls, voting cards, ballots and other election material), disseminating voter information about the electoral process, and developing and maintaining election-related IT systems to process the results. Campaign oversight, election-related social media activity, voter education and calls to vote are not part of its responsibilities. Any illegal activity is the responsibility of the security agencies or the public police.

Use of ICTs

Elections in Sweden are mostly administered manually. All key elements of the electoral process are paper based; technology is only used to increase efficiency. However, more technology is seen as unavoidable in future elections.

Digital tallying is only conducted as a parallel, redundant system. The Elections Authority utilizes a central IT system for the transmission and tabulation of results and seat allocation. This system is the main asset under its authority. An additional digital system provides the media with election results.

The tax agency supplies data on all residents for the creation of voters' lists, and provides the Elections Authority with its website and related infrastructure. The Elections Authority currently has no significant social media presence.

Risks

All election-related ICT systems are continuously maintained with industry-level security standards at all times; additional security is not needed for election periods. Low-level cyberattacks, such as DDoS, are expected any time, even between elections, and have no impact on the agency or its systems. Continuity plans for system breakdowns are in place and a complete fallback on manual, paper-based procedures is possible at any time.

A high emphasis is placed on data protection, as data losses and leaks are even more difficult to recover from than system breakdowns. Cyber-risks are therefore closely linked to information security, in the form of both data breaches and disinformation. Protecting systems at the municipal level is another focus area, given the limited resources available at this level.

Interagency collaboration

All Swedish authorities receive written instructions from the government every year that clearly define all of their responsibilities. While elections are not explicitly recognized as such, they have been increasingly recognized as critical national infrastructure since 2017. As a result, close collaboration on securing the electoral process between election-related agencies has been facilitated by the Swedish Civil Contingencies Agency, which is responsible for civil protection, public safety, emergency management and civil defence as long as no other authority has responsibility. Responsibility refers to measures taken before, during and after an emergency or crisis.

Interagency cooperation is an essential part of protecting the electoral process from cyber-risks. While cooperation between the 312 local election authorities is long-standing practice, the increased need to coordinate with security agencies and other actors is a new development.

The Civil Contingencies Agency is tasked with countering any influence activities designed to disrupt, interfere with or manipulate elections. It collaborates with multiple actors including the Election Authority, intelligence services, security police, public police, local police, all election administrations at the county and local levels, the tax agency, transportation agency and the media.

The agency's counterinfluence project consists of several stages:

- threat assessment (identify possible influence activities, assess vulnerabilities and risks, identify key actors);
- developing methods and recommendations to counter influences, increasing awareness of authorities (informing and training relevant authorities, informing the public);
- supporting cooperation between authorities (to diminish vulnerabilities);
- increasing public awareness (to diminish the effects of influence activities);
- establishing an organization to monitor, identify and counter influence activities during an election; and
- developing communication strategies and prepared narratives.

Crisis management relies on the principle of responsibility of strong autonomous authorities: 'Whoever is responsible for an activity in normal conditions, shall maintain that responsibility in a crisis situation.' Those authorities are supported by the Civil Contingencies Agency through a common situational overview, information sharing and coordinated decision-making. The agency monitors the situation and publishes confirmed multi-agency information through multiple channels, including a website and various social media outlets as the primary communication channel for citizens to access all relevant information.

Coordinated information sharing is important to avoid conflicting messages, an information vacuum and an undermining of trust. Interagency cooperation therefore ensures that all agencies are always fully informed about the current situation and share the same message regarding cyberthreats.

Interagency collaboration involves regular high-level meetings between participating organizations. While in the past some agencies were reluctant to cooperate or share information, they now understand the importance of such cooperation and are very open and supportive of it. Cooperation initiated for election-related issues has also been useful in other governance areas.

Significant emphasis is placed on transparency and maintaining a well-informed electorate and a well-prepared media. All agencies transmit a unified message that the Swedish process is decentralized, largely manual, and therefore very robust and well protected against cyberattacks. The manual process helps to mitigate concerns about cyberthreats, but has also created a need to explain why elections remain low-tech in a country where almost everything else is digital.

The overall aim is that any actual or alleged cyberincidents do not come as a surprise to the public and that the robustness of the systems is well known in advance.

Ukraine

Structure of the EMB

The Central Elections Commission (CEC) of Ukraine is a permanent, independent state body that supervises and conducts presidential, parliamentary and local self-government elections as well as referendums. The electronic voter register is updated by local state register authorities that operate independently of the CEC.

Use of ICTs

The following technologies are used for elections in Ukraine:

- the electronic State Voter Register;
- the Unified Information Analytical System ‘Elections’, an election management system supporting various stages of the electoral cycle including result transmission and tabulation systems, candidate registration, campaign finance reporting, observer registration, signature collection system for citizen initiatives and related document workflows; and
- the CEC website.

Risks

During the 2014 presidential and parliamentary elections, a series of simultaneous cyberattacks took place. The transmission of results by district electoral commissions was disrupted, malware and phishing attacks occurred, and DDoS and defacing attacks were launched against the website that displayed the election results. Similar DDoS attacks against the CEC were launched again ahead of the 2019 presidential elections.

These past attacks highlight the following key cyberthreats:

- massive attacks aimed at breaking into internal and public network resources;

- malicious software with the help of insiders or phishing techniques; and
- DDoS attacks at core election infrastructure and public websites.

While there are clear suspicions about the perpetrators, finding hard evidence is difficult and the identity of the attackers is still not known.

Major cyber-risks are related to voter lists, the publication of election results, disinformation activities aimed at undermining trust in elections, voter suppression and reducing voter turnout:

- compromising the data and systems, in order to make it difficult or impossible to implement the electoral procedures, for example creating conditions for temporary delays during elections in regions;
- unauthorized modification of voter registration data to compromise voter lists and create conditions to appeal the election results; and
- distorting information or blocking access to resources, including the results process, to discredit electoral bodies and their ability to secure the electoral process, and create opportunities to place fake messages about election results and reduce voters' trust and turnout.

Interagency collaboration

Efforts are focused on strengthening the CEC's technical capabilities to protect electronic registers and databases, and the information and telecommunication system they rely on, from cyberthreats and challenges. Interagency collaboration on election cybersecurity occurs primarily between the CEC and the Security Service (Ukraine's main body responsible for cybersecurity), which dates back to 2010 and intensified after the 2014 attacks. For the 2019 elections, the Security Service was supported by the NATO–Ukraine Trust Fund on Cybersecurity to strengthen the CEC's technical capabilities to protect it from cyberattacks.

The CEC and Security Service collaborate on a daily basis. They have formed a joint commission for the common project and work together at both the technical and senior levels. The Security Service provides both hardware and technical expertise to the CEC.

In addition, the Cyber Department of the National Police of Ukraine, State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and the Security Service, as well as state enterprises and private contractors, are involved in the development, certification and protection of election-related ICTs. Before they are used by the CEC, election-related information systems undergo state assessment to receive a certificate of compliance. This entails approval of the terms of references and documentation by the SSSCIP, preliminary testing, and an assessment of the system's conformity with the terms of reference and information protection requirements. During their use, SSSCIP experts monitor the systems and protect them from attacks.

In 2018 Ukraine updated its list of critical infrastructure to specify which assets the government assumes responsibility for protecting. The CEC is responsible for all public communication on cyberprotection in elections.

United Kingdom

Structure of EMB

Elections in the United Kingdom are run locally by independent returning officers based in each local authority, and in Northern Ireland by the chief electoral officer. They are overseen by an independent regulator, the UK Electoral Commission, which is responsible for party registration, regulation of political party financing, research, developing standards, and supporting elections and referendums in the UK. While the government is responsible for electoral policy and changes to the law, the commission feeds into this through reports and wider policy work.

Use of ICTs

The UK does not offer online voting. Voter registration is the responsibility of local electoral registration officers and there is no central voter register. While voting and vote counting are manual processes, several ICT applications are in place:

- a system for submitting online applications to register to vote with local authorities;
- elections management software that supports the administration of registers and elections;
- a party finance returns database including an online submission system; and
- result collation software developed for the 2016 EU Membership Referendum.

Risks

The online voter registration system is located on the UK's e-government website, which is maintained by the Government Digital Service as part of the Cabinet Office. This voter registration system is becoming increasingly popular among citizens. As it is available via a public website, it is potentially exposed to attacks. Safeguards and fallback options include a manual alternative of traditional registration with local electoral registration officers and additional checks based on the need to submit personal details to use the system.

The electoral management systems used by local authorities are developed by four different providers. The main risks for offline systems include ransomware, malware and the illegal publication of personal data. While there have been no reported incidents, the National Cyber Security Centre (NCSC) has issued guidance to local authorities, including on the organization's security, staff behaviour and awareness. Most data are held separately by local authorities, which limits the scope for harm by individual attacks.

The electronic result collation system, initially established for the 2016 EU Membership Referendum, has a paper-based backup that runs in parallel. Election data feeds for media and other outcome reporting channels also form a potential risk factor.

For political parties, the main risk factors are leaking of personal data of high-profile individuals and supporters, and malware and ransomware.

As little of the electoral process is digital, cyberthreats have thus far had, apart from some conspiracy theories, limited impact on voter confidence, and elections have not been designated as critical infrastructure in the UK. Yet the manual process is not risk free: mistakes can happen and the postal voting process can be problematic; there have been past allegation of tampering with mail.

An overall challenge for the Electoral Commission and the NCSC is the changing nature of cyberthreats and adversaries. Solutions need to be found to handle new threats as they emerge in a fast-changing environment. Therefore, the definition of cyber-risk differs from election to election.

Many cyber-related challenges relate to digital campaigning, micro-targeting and the implications for social media companies, parties and the government, including the need for more powers for the Electoral Commission to access information, enforce rules and sanction perpetrators.

Interagency collaboration

In the UK, the responsibility to protect elections against cyber-risks falls under the mandate of a broad range of agencies in addition to the Electoral Commission, including the NCSC, the Information Commissioner, the Constitution group in the Cabinet Office (especially in the run-up to elections), the National Crime Agency and the police.

The security of the various ICT applications as outlined above is the primary responsibility of the holder of the application, which in many cases are local administrations. The UK Electoral Commission is therefore not immediately responsible for many cyber-risks. However, in case of problems, even at the local level, attention automatically focuses on the Electoral Commission since it is the most visible election agency. While the commission cannot (and does not) protect local administrations, it can make recommendations if there is a failure in the local security system.

The Electoral Commission has collaborated with the NCSC since 2016, after reports of foreign interference in the US elections appeared. Since then, the NCSC has taken up an informal but important role in coordinating with the Electoral Commission and the Constitution group at the Cabinet Office. Given that its formal tasks are to provide both guidance and incident management support, its role with regard to elections is to compile electoral risks and to provide guidance to these bodies. The main focus of the NCSC is general elections, although it also supports local elections. Interagency meetings take place on an ad hoc basis, as required and if risks are discovered, with more frequent meetings closer to elections. At the local level, the NCSC also provides a manual on cybersecurity for returning officers and advises the association of electoral administrators.

Digital campaigning by political parties and false/misleading information on social media are of significant concern to the Electoral Commission. Although they do not fall under its immediate mandate, closely related concerns, such as voter confidence and party financing (including funding of digital campaigns) do. Hence, the commission makes legislative recommendations in this domain.

The commission's jurisdiction is limited to UK territory. It considers foreign interference in the electoral process to be the primary responsibility of the national security agencies. Oversight related to the use of citizens' personal data and data integrity fall in the domain of the UK Information Commissioner.

The NCSC and the Centre for the Protection of National Infrastructure have produced briefings, guidance and information on good cybersecurity practices for the systems that support the delivery of UK elections. This includes guidance for political parties on the risks of data breaches, including phishing or spear-phishing attacks, and providing evidence of recent attempts. The NCSC also regularly briefs political parties and candidates, under a strict protocol to avoid political sensitivities, to remind them of cybersecurity risks. The NCSC also engages with broadcast media on cybersecurity issues.

High-profile cybersecurity concerns and an active interest in elections has led to good cross-government and interagency collaboration. Given the Election Commission's limited mandate and the fact that many different agencies have election-related responsibilities, partnerships and collaboration with other agencies are very important.

While it is generally clear what each organization does, their responsibilities are not codified in laws and procedures. The Election Commission has therefore had to develop a good understanding of the role of each organization.

Collaboration has grown organically over time, and is largely informal. It takes place in the form of individual meetings, regular dialogue, information sharing and contingency planning between the agencies. There is close cooperation between the Electoral Commission and the Information Commissioner.

As all actors are rarely around one table, the UK Elections Commission plays an important role in orchestrating this information exchange. Since overprescribing may not be suitable in such a scenario, the commission can offer advice and expertise, and make sure the right messages are communicated publicly.

For public communication purposes, the Electoral Commission has established approaches on how to manage election-related incidents and how to deliver messages that enhance the trust of citizens, who expect fast and credible responses.

While the Electoral Commission does not have dedicated staff responsible for cyberthreats, a small team is available to respond to social media-related issues and regularly communicates with social media providers.

The lead for responding to incidents depends on the type of threat. A few specific election security exercises have also been held. Overall, the willingness to cooperate depends on the threat, but is limited outside election periods. The security services responsible for risk assessments need to decide where to invest their resources and will only respond if they deem the risk severe enough.

United States of America

Structure of EMB

The United States has a non-uniform election administration, with more than 8,000 independently operating election jurisdictions at the local and state levels. This structure allows jurisdictions to specialize their processes to best serve the local communities. In the face of cyberthreats, multiple US federal intelligence officials identified the non-uniform nature of US elections as a security asset.

The US Electoral Assistance Commission (EAC) is an independent, bipartisan resource on election administration, established after the passage of the Help America Vote Act of 2002. The EAC serves as a clearinghouse of election administration data, tool kits and training materials. It also administers the National Voter Registration Form and the voting machine testing and certification programme. It produces the Voluntary Voting System Guidelines, which is the only national voting system standard, and acts as the federal representative for election administrators in the Council of State Governments. Key tasks of the EAC are to maintain voter confidence and provide guidance to vendors.

Use of ICTs

A diverse range of election technologies have been deployed across the USA, in part because the Help America Vote Act triggered technology investments. More than 10 years later this ageing technology created increasing vulnerabilities, the need for renewed investment in upgrades and replacement, and even calls to return to paper-backed systems that in turn would recreate previous challenges, for example related to the chain of custody and accessibility.

Election officials must now find ways to extend the life of voting technology while holding the systems to the highest standards possible and in spite of the limited funds available to build preventative measures that can withstand and recover from attacks. There is also limited funding to update systems and develop additional security expertise. Greater security measures and higher system standards cannot come at the expense of limiting accessibility for voters with disabilities, voters who need language assistance, or those serving in the military or living overseas. In 2018, USD 380 million was made available for system updates to be distributed over five years based on each state's population.

Risks

Due to the structure of the US election administration, the definition of cyber-risks and responsibilities is multi-faceted and depends on the actor. State and local jurisdictions are responsible for their own data and technology. Three systems are particularly important in this regard:

- voter registration systems;
- voting machines and related technologies; and
- reporting and tabulation systems.

Previous experience shows that compromising voting machines on a large scale is not necessarily the main concern. Manipulation of voter registers is a higher risk as those systems are often online and connected to the databases of various institutions. This makes protecting voter data against breaches and manipulation a key priority.

While voting technology vendors are expected to secure their technology, the need for more credible security was underscored at the 2017 and 2018 DefCon conferences, where several examples of election technologies were publicly compromised by white hat hackers. While some of the hacks happened under very unrealistic conditions, they highlighted the expectations for technology providers to respond to such claims and, where needed, adjust their systems.

An overall cyber-risk is the loss of voter confidence, even if only based on rumours. If voters assume an election's credibility has been compromised, they are less inclined to participate.

The First Amendment of the US Constitution guarantees the freedom of speech, which exempts social media from EMB regulation or oversight. However, there are close partnerships with providers such as Google and Facebook on the development of better self-regulation. Voters must therefore be aware of their responsibilities, including to inform themselves about influence operations and the need to verify data and information. The EAC provides information videos online to inform voters of their responsibility to uphold electoral integrity (EAC 2018).

Interagency collaboration

The EAC is a partnership-driven agency that collaborates with diverse institutions, including the Department of Homeland Security (DHS), the National Institute of Standards and Technology, the Department of Defense, the US Postal Service, the National Association of State Election Directors, the National Conference of State Legislatures, the Federal Bureau of Investigation, the National Security Agency and public policy research institutions. It also cooperates with the private sector and election technology providers.

Collaboration between the EAC and the DHS started before the 2016 election and helped the DHS communicate security information to election officials and administrators, and to understand elections and election administrators' feedback. In 2017 the DHS designated elections as critical infrastructure. This designation shapes how the federal government views and interacts with a sector and prioritizes the allocation of security resources. For example, it allowed the involvement of the DHS and its massive security capacity, including 240,000 staff, to provide support to election administrators in areas from risk identification to the provision of cybersecurity advice.

Local election officials initially had reservations about cooperating with federal officials, particularly from the DHS. The EAC, which represents all election administrators, played an important role in legitimizing DHS cooperation. Another challenge has been the timely and useful transfer of information between election officials. The Multi-State Information Sharing Analysis Center has created an information-sharing pilot programme that will allow owners and operators of election technology to better secure their systems against cyberthreats (Hicks 2018).

Coordinated interagency collaboration is organized in two mayoral forums. The EAC is represented in both and was instrumental in setting them up:

- The Elections Government Sector Coordination Council brings local, state and federal EMBs together every two months to exchange information and plan for cyber-resilience with DHS support. This cooperation is largely formalized and official protocols for disseminating information have been established.

- The Sector Coordinating Council brings together a broad range of private actors, from technology vendors to media representatives. The council is self-organized and meets about twice a month in a joint call.

A challenge in cooperation with the private sector is that in the wake of cybersecurity concerns, many small companies emerged that need to be legitimized, which created a new role for both the DHS and EAC.

The US electoral process relies on a large number of polling officials who are not always aware of how to keep technology secure. The EAC therefore offers training to ensure election officials are able to respond to cyberattacks. In cooperation with the Belfer Center training exercises were created that condense six months of work around elections into scenarios that can be practised in three hours.

References and further reading

Australian Electoral Commission, 'Electoral Backgrounder: Electoral Communications and Authorization Requirements', 23 April 2019, <https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm>, accessed 10 October 2018

—, 'How the Senate result is determined', <https://www.aec.gov.au/Voting/counting/senate_count.htm>, accessed 11 October 2018

Australian Government Attorney-General's Department, 'The Protective Security Policy Framework', [n.d.], <https://www.protectivesecurity.gov.au/Pages/default.aspx>, accessed 10 October 2018

Australian Government Cyber Security Centre, 'Information Security Manual', [n.d.], <https://acsc.gov.au/infosec/ism/>, accessed 10 October 2018

Australian Government Department of Home Affairs, *Cyber Security Strategy* (Commonwealth of Australia, 2016), <https://cybersecuritystrategy.homeaffairs.gov.au/>, accessed 10 October 2018

Australian Government, *International Cyber Engagement Strategy* (2017), <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, accessed 10 October 2018

Bay, S. and Šnore, G., *Protecting Elections: A Strategic Communications Approach* (Riga: NATO Strategic Communications Centre of Excellence, 2019), <https://www.stratcomcoe.org/protecting-elections-strategic-communications-approach >, accessed 23 May 2019

Belfer Center for Science and International Affairs, Harvard Kennedy School, *The Cybersecurity Campaign Playbook*, Defending Digital Democracy, 20 November 2018a, <https://www.hks.harvard.edu/publications/cybersecurity-campaign-playbook>, accessed 21 August 2017

Belfer Center for Science and International Affairs, Harvard Kennedy School, NDI and IRI, *The Cybersecurity Campaign Playbook, European Edition*, November 2018b, <https://www.ndi.org/sites/default/files/european_campaign_playbook_-_web.pdf>, accessed 21 August 2017

Canada Government Communications and Security Establishment (CSE), *Cyber Threats to Canada's Democratic Process*, 2017, <https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf>, accessed 8 May 2018

—, *2019 Update: Cyber Threats to Canada's Democratic Process*, 2019, <https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf>, accessed 16 April 2019

DefCon, *DEFCON 25 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf, accessed 16 October 2018

—, *DEFCON 26 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2018, <https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf>, accessed 16 October 2018

Elections Canada, 'Roles and Responsibilities of Government Agencies and Elections Canada', [n.d.], <http://www.elections.ca/content.aspx?section=vot&dir=bkg/sec&document=legal&lang=e>, accessed 6 February 2019

European Commission (EC), *Election Interference in the Digital Age, Building Resilience to Cyber-enabled Threats* (Brussels: EC, 2018a), <https://ec.europa.eu/epsc/publications/other-publications/election-interference-digital-age_en>, accessed 9 November 2018

—, *Recommendation on Election Cooperation Networks, Online Transparency, Protection against Cybersecurity Incidents And Fighting Disinformation Campaigns in the Context of Elections to the European Parliament* (Brussels:

EC, 2018b), <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf>, accessed 6 November 2018

—, *Action Plan on disinformation: Commission contribution to the European Council* (Brussels: EC, 2018c), <https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en>, accessed 17 June 2019

—, *Code of Practice on Disinformation* (Brussels: EC, 2018d), <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>, accessed 17 June 2019

—, *EU Member States Test their Cybersecurity Preparedness for Fair and Free 2019 EU Elections* (Brussels: EC, 2019), Press Release, <http://europa.eu/rapid/press-release_IP-19-2011_en.htm>, accessed 5 April 2019

European Union, *Directive on Critical Information Systems* (Brussels: EU, 2016), <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, accessed 6 November 2018

—, *Code of Practice on Disinformation* (Brussels: EU, 2018), <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454>, accessed 9 November 2018

Financial Review, 'Australian Electoral Commission strengthens defenses against foreign hacking', 30 April 2018, <https://www.afr.com/news/australian-electoral-commission-strengthens-defences-against-foreign-hacking-20180430-h0zfzz>, accessed 10 October 2018

Finland Prime Minister's Office, 'Central Government Communications Guidelines', (Helsinki: Finland Prime Minister's Office, 2016), <https://vnk.fi/en/central-government-communications-guidelines>, accessed 10 October 2018

G7, 'Commitment on Defending Democracy from Foreign Threats' (Charlevoix: G7, 2018), <https://www.mofa.go.jp/files/000373846.pdf>, accessed 20 June 2018

The Guardian, 'Electoral watchdog powerless to crack down on offshore political ads targeting Australians', 24 July 2018, <https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>, accessed 11 October 2018

Hicks, T., ‘Defending and recovering American election systems’, *Brown Journal of World Affairs*, 24/2 (2018), <http://bjwa.brown.edu/24-2/defending-and-recovering-american-election-systems/>, accessed 20 June 2019

INE, Twitter–Instituto Nacional Electoral Memorandum of Cooperation, 11 June 2018, <http://centralelectoral.ine.mx/wp-content/uploads/2018/03/Memorandum-de-Entendimiento-con-Twitter.pdf>, accessed 6 November 2018

International Foundation for Electoral Systems (IFES), *Social Media, Disinformation and Electoral Integrity* (IFES 2019), white paper, forthcoming, <https://www.ifes.org>

IP-Watch, 'A Digital Geneva Convention: Nobel Prize-Worthy or Dangerous?', 19 December 2017, <http://www.ip-watch.org/2017/12/19/digital-geneva-convention-nobel-prize-worthy-dangerous/>, accessed 10 October 2018

Microsoft Policy Papers, *A Digital Geneva Convention to Protect Cyberspace* (Redmond, WA: Microsoft, 2017), <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>, accessed 8 May 2018

NIS Cooperation Group, *Compendium on Cyber Security of Election Technology* (CG Publication: 2018), <http://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf>, accessed 11 October 2018

Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights (OSCE/ODIHR), *International Election Observation Mission North Macedonia, Presidential Election*, April 2019, <https://www.osce.org/odihr/elections/north-macedonia/417818?download=true>, accessed 23 May 2019

Parliament of the Commonwealth of Australia, *Status Report of the Joint Standing Committee on Electoral Matters*, March 2019, <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024259/toc_pdf/Statusreport.pdf>, accessed 14 April 2019

Past, L., ‘All elections are hackable: scalable lessons from secure i-voting and global election hacks’, *European Cyber Security Journal*, 3/3 (2017), pp. 34–

47, <https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF>, accessed 8 May 2018

Poynter Institute, *A Guide to Anti-misinformation Actions around the World* (2018), <https://www.poynter.org/news/guide-anti-misinformation-actions-around-world>, accessed 8 May 2018

Republic of Estonia, 'Information System Authority', [n.d.], <https://www.ria.ee/en.html>, accessed 11 October 2018

United States Department of Homeland Security, *National Cyber Incident Response Plan* (Washington, DC: DHS, 2016), <https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf>, accessed 11 November 2018

United States Electoral Assistance Commission (EAC), *Election Security Preparedness*, [n.d.], <https://www.eac.gov/election-officials/election-security-preparedness/>, accessed 11 November 2018

—, 'Election Security Video', <https://www.eac.gov/electionsecurity/>, accessed 11 November 2018

—, *Starting Point: U.S. Election Systems as Critical Infrastructure* (Silver Springs, MD: USEAC, 2017), <https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf>, accessed 8 May 2018

El Universal, *Facebook – Instituto Nacional Electoral Memorandum of Cooperation*, 2018, <http://interactivo.eluniversal.com.mx/graficos/online/pdf-18/convenio-facebook.pdf>, accessed 6 November 2018

Verificado, *Noticias Falsas* (2018), <https://verificado.mx/categoria/noticias-falsas>, accessed 15 April 2019.

Wolf, P., *Cybersecurity and Elections: An International IDEA Round-table Summary* (The Hague: International IDEA, 2017), <https://www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary>, accessed 8 May 2018

About the authors

Sam van der Staak is the Head of International IDEA's Europe Programme, which involves advising political parties, electoral commissions and other state institutions on a broad range of democratic reforms. He is the author of publications on topics including political party development, citizen movements and political finance, and is a regular commentator for various European media. Prior to his involvement in democracy assistance, he worked in the Netherlands House of Representatives.

Peter Wolf is Technical Manager for Electoral Processes at International IDEA. His research and work focus on ICTs in elections and democracy, with a special emphasis on sustainable and trusted applications of technology in electoral processes. He has many years of international assistance experience and is the author of numerous publications in this field.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with the mission to advance democracy worldwide, as a universal human aspiration and enabler of sustainable development. We do this by supporting the building, strengthening and safeguarding of democratic political institutions and processes at all levels. Our vision is a world in which democratic processes, actors and institutions are inclusive and accountable and deliver sustainable development to all.

What do we do?

In our work we focus on three main impact areas: electoral processes; constitution-building processes; and political participation and representation. The themes of gender and inclusion, conflict sensitivity and sustainable development are mainstreamed across all our areas of work.

International IDEA provides analyses of global and regional democratic trends; produces comparative knowledge on good international democratic practices; offers technical assistance and capacity-building on democratic reform to actors engaged in democratic processes; and convenes dialogue on issues relevant to the public debate on democracy and democracy building.

Where do we work?

Our headquarters is located in Stockholm, and we have regional and country offices in Africa, the Asia-Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<http://idea.int>

Information and communication technologies are increasingly prevalent in electoral management and democratic processes, even for countries without any form of electronic voting. These technologies offer numerous new opportunities, but also new threats. Cybersecurity is currently one of the greatest electoral challenges. It involves a broad range of actors, including electoral management bodies, cybersecurity expert bodies and security agencies.

Many countries have found that interagency collaboration is essential for defending elections against digital threats. In recent years significant advances have been made in organizing such collaboration at the domestic and international levels.

This guide tracks how countries are making progress on improving cybersecurity in elections. Based on an extensive collection of 20 case studies from all over the world, it provides lessons for those wanting to strengthen their defences against cyberattacks.

International IDEA
Strömsborg
SE–103 34 Stockholm
Sweden
Telephone: +46 8 698 37 00
Email: info@idea.int
Website: <http://www.idea.int>

ISBN: 978-91-7671-255-9 (PDF)