Elections and the Challenge of Cybersecurity

Literature Review and Analysis of the Electoral Cycle

Submission date: October 22, 2021

International Foundation for Electoral Systems (IFES)

DRAFT

DRAFT

Contents

Executive Summary 1

I. Introduction 2

II. Cybersecurity in Elections: A Brief History and Overview of the Literature 4

A. International, Regional and Domestic Standards for Cybersecurity in Elections 6

B. Good Practice Guidelines for Implementing Election Technology 9

C. Cybersecurity Instruments and Frameworks 10

D. Election Observer Guidelines 11

E. Academic literature 12

III. Integrating a risk-based lens to understand election cybersecurity 15

A. Threat Actors 19

1. Foreign State Actors and APTs 20
2. Government Actors 21
3. Criminal Groups 21
4. Insider threats 22

IV. Election Stakeholders 22

A. Multi-stakeholder coordination 22

B. Civil Society Organizations 23

C. Political Parties 25

V. The Electoral Cycle 26

A. Pre-election Period 28

1. Legal and Regulatory Context 28
2. General election administration and planning 32
3. Boundary delimitation 33
4. Voter registration 34

DRAFT

5. Candidate Registration Process 35
6. Strategic communications 36
7. Voter information and education 37
B. Election Period 38
1. Voting process 38
2. Counting at the polling-station level 40
3. Results transmission, tabulation and reporting 41
C. Post-Election Period 43
1. Electoral dispute resolution process 43
2. Detecting, investigating and prosecuting cybercrime in elections 44
V. Conclusions 46
Annex A: List of relevant publications or resources 48
A. International, Regional, and Domestic Standards 48
B. Practitioner Publications 48
C. Cybersecurity Instruments and Frameworks 50
D. Election Observer Guidelines 50
E. Academic Literature 51
F. Jurisprudence 52
G. Other Reports 52
DRAFT

1. Executive Summary

Since electronic voting technology was first introduced, a variety of new technologies have been developed and integrated into elections around the world, affecting each step of the election process. In many cases, these technologies are efficient, reduce the risk of human error,[1] improve accessibility of elections[2] and can mitigate or prevent some types of election fraud.[3] Yet, rapid growth in the use of election technology has increased the potential for disruptive cyber attacks.[4] As election management bodies (EMBs) have taken up new technologies – particularly around digitization of voter registries, transmission processes and aggregation of election results - multiple sources of policy, principle and practice in electoral cybersecurity have emerged. However, significant gaps remain in developing further guidance and regulation for EMBs, policymakers, and electoral stakeholders to ensure that electoral technology is secured from threats and trusted by the public.

In part, these gaps exist because a static approach to managing these threats is insufficient in any arena, including the electoral process. As the number of election technology applications grows, elections have begun to attract the attention of a wider spectrum of threat actors. There are well known examples of cyber attacks on elections launched by well-resourced foreign state actors with the aim of undermining trust in democratic processes and the legitimacy of their outcomes. Domestic actors have also emerged to threaten elections. They may be politically, financially, or ideologically motivated, and operate individually or collectively, but like their foreign counterparts they are finding ways to undermine trust in elections. The emergence of these domestic actors means that institutions charged with upholding the integrity of elections must also work to recognize and mitigate potential insider threats.

DRAFT

While such responsibilities traditionally fell within the purview of the national security sector, the range of stakeholders that are being targeted with cyber attacks – and are working to prevent and respond to them – is expanding. For instance, EMBs have taken up a role in risk analysis, mitigation and response to threats against their systems and equipment. Civil society organizations, political parties, and candidates have also been targeted by threat actors that are driven by distinct motives. Each stakeholder group must assess their own specific vulnerabilities and develop and take ownership of a cyber mitigation strategy.

Holistic analysis of the full electoral cycle can reveal insights into how this expanding range of stakeholders can understand, prioritize, and mitigate such threats. Effective cyber threat detection and mitigation is characterized by a continuous and well-defined process of risk management that hews to industry best practices defined in several standard risk management frameworks. While governments and industry have widely adopted and typically follow these

[1] The Rationale for E-voting in Brazil | National Democratic Institute (ndi.org)

[2] A Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment (nist.gov)

[3] India's electoral democracy: How EVMs curb electoral fraud (brookings.edu)

[4] The attacks on Ukraine in 2014 and the United States in 2016 are particularly illuminating. See, for instance, Martin-Rozumilowicz and Chanussot (2019).

frameworks, adherence is often limited by resource availability, competing priorities and lack of cybersecurity advocacy.

This report uses the electoral cycle as a heuristic to map risks and mitigation activities that EMBs and their partners might face during pre-election, election and post-election periods. By understanding the wide range of potential risks and threats they may face throughout an election cycle, EMBs will be better able to prioritize where to expend their resources and how to adapt existing risk management frameworks and cybersecurity good practices to their context.

It should be noted that many EMBs will not be able to address escalating cyber attacks on their own. Information technology is used across the entirety of an election cycle, and is owned, maintained, and used by a variety of actors – from software and hardware providers, candidates and other institutions that play a role in election administration. Yet, because the activities performed across the electoral cycle are interrelated, security compromises or breaches to one involved stakeholder can have wide-reaching effects. Considering this reality, EMBs will need to work with other stakeholders (such as state offices that compile civil registries from which voters lists may be pulled, or authorities auditing voting machines) to establish mature cybersecurity postures to holistically recognize and manage the risks individually and collectively across the electoral cycle.

In particular, a review of recent trends indicate that EMBs and their partners may face particular challenges when it comes to protecting voter registration databases and results tabulation and transmission systems – which are attractive targets for cyber attacks to undermine stakeholder acceptance of electoral outcomes. Voter register databases and functions can increasingly be accessed online by members of the public — either to simply check registration status, or to execute voter registration or absentee ballot requests. This ease of access must be balanced with the risk that such resources may be compromised by malicious actors undermining the election process.

DRAFT

These risks can be further compounded by poor cyber hygiene among institutions and users involved in administering and maintaining election technology, along with *ad hoc* and piecemeal approaches to cybersecurity involving third parties, technology procurement and multi-stakeholder collaboration.

I. Introduction

The process of planning for and administering democratic elections is one of the most complex, collaborative endeavors a country may undertake. The institutional context within which an election is managed and executed varies across many different democratic arrangements, but the core institution charged with administering a country's election process is commonly referred to as an eElection mManagement bBody (EMB). The EMB has multiple responsibilities, including maintaining integrity throughout the planning process, carrying out elections, and finalizing results.[5] The continued integration and use of information technology within the broader process of electoral planning, management and execution is both necessary and desirable. As such, an EMB's mandate to protect the integrity of an election naturally extends to ensuring adequate cybersecurity for the information technology utilized across the spectrum of activities under its purview. The term "cybersecurity" refers to the means through which electronically processed information can be secured against disruption, disablement, destruction or malicious control, thus protecting against the possibility of the information's integrity, availability or confidentiality becoming compromised.[6] The use of cyber-based attacks against public institutions – including those associated with election infrastructure – are a known and documented occurrence, and one that has occurred with increasing frequency, as noted in the next section.

DRAFT

A 2020 report by the Venice Commission noted that "greater efforts need to be undertaken to prosecute [election-related, cyber-based] interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections."[7] The Venice Commission also exhorted States parties to practice international judicial and law enforcement cooperation in investigating and prosecuting cyber crime, as States had committed under the 2001 Budapest Convention.[8]

Elections all over the world have become targets of cyber attacks; in addition to the incidents mentioned below, there are examples across Europe, North America, Latin America,[9] Africa,[10] Asia,[11] and Oceania.[12] Citizens are generally aware that these attacks are likely, and many doubt

[5] For a comprehensive overview of the various institutional arrangements associated with the management of democratic elections, see the International Institute for Democracy and Electoral Assistance (IDEA) Electoral Management Design Revised Ed. (2014) available at: https://www.idea.int/sites/default/files/publications/electoral-management-design-2014.pdf

[6] National Institute for Standards and Technology (NIST) https://csrc.nist.gov/glossary/term/cybersecurity and https://csrc.nist.gov/glossary/term/cyber_attack

[7] https://rm.coe.int/electoral-dispute-resolution/16809f0007 page 107

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?module=signatures-by-treaty&treatynum=185

[9] https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democratic-elections-latin-america

[10] https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

[11] https://www.fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html

– with good reason – that their respective countries are prepared to successfully counter them.[13] Recent elections in Kenya and the Democratic Republic of the Congo, for instance, have seen electronic results seemingly disappear into thin air — even without suspected external interference. Such self-inflicted cyber failures expose the need to enhance electoral technology security and reliability, improve user knowledge and training, introduce additional safeguards, and promote standard practices to reduce overall cybersecurity risks.

There are differing opinions as to whether election technology – especially electronic voting and results management devices – can be fully protected from cyber attacks. While some EMBs (such as Brazil's TSE[14]) and technology vendors, as well as successful electoral candidates, may insist that election technology can be fully protected, cybersecurity experts generally agree that there is no way to guarantee an absolute level of security against cyber threats and fully protect against all risks. While cybersecurity risks cannot be eliminated entirely, many can be mitigated with the application of security controls as part of a holistic cybersecurity strategy.

This report sets aside the myth of impenetrability to investigate the more practical threat the concept of cybersecurity as a risk management process that should be adopted by EMBs. The paper begins with an overview of technology and cybersecurity in elections and a brief literature review of the existing body of work that informs electoral cybersecurity policy and practice. Next, the report introduces the key cybersecurity concepts of risk management and security control mechanisms and applies them to the electoral process using a risk-based approach.

DRAFT

Finally, the paper discusses the primary actors posing cyber threats to election technology; the cyber vulnerabilities different election stakeholders encounter; and the election technology used, associated risks, and effective mitigation strategies across all stages of the electoral cycle. The briefing will conclude with a discussion of areas where further analysis and guidance is needed to strengthen the cybersecurity postures of electoral management bodies.

II. Cybersecurity in Elections: A Brief History and Overview of the Literature

Traditional, manual voting and hand-counting paper ballots has dominated elections since the mid-1800s. In 1964, electronic voting technology was first introduced with punch cards and computer tally machines, used in two counties in the U.S. state of Georgia during presidential primaries.[15] Since then, a variety of new technologies have been developed and integrated into

---

[12] https://www.smh.com.au/politics/federal/cyber-attacks-on-elections-growing-amid-concern-for-australia-s-political-parties-20201028-p569fg.html

[13] Poushter, J. ; Fetterolf, J. (January 9, 2019). International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security. Pew Research Center. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[14] https://www.telesurtv.net/news/brasil-tse-respalda-sistema-voto-electronico-20210802-0026.html

[15] International Foundation for Electoral Systems. (2014, November 20). Electronic Voting Machines Pakistan Factsheet. p. 1. https://www.ifes.org/sites/default/files/electronic_voting_machines.pdf; Fischer, E. (2003). Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. Congressional Research Service. https://crsreports.congress.gov/product/pdf/RL/RL32139/3; Tokaji, D. (2005). The Paperless Chase: Electronic Voting

elections around the world, affecting each step of the process down to casting and tabulating ballots. In the wake of the 2000 general elections in the United States, punch-card voting machines were replaced by optical scanners for reading paper ballots and voting machines that included comprehensive systems to receive and record voter inputs, encrypt the data, and transmit and tabulate results. In many cases, introducing such technology decreased the time to count ballots and reduced the quantity and cost of staff needed to tabulate results, as well as the risk of human error.[16] Some machines also improved accessibility for persons with disabilities[17] and prevented certain forms of election fraud such as stuffing ballot boxes and ballot theft.[18]

But the uptake of technology in election processes has not been consistent or linear. Nearly 60 years since the introduction of the first punch cards, election technology is far from ubiquitous, especially when it comes to polling. While most countries have been increasing their use of technology solutions in voter registration and results transmission – for example, on the African continent where biometric voter verification machines have been introduced in Kenya and Ghana, biometric voter registration in Zimbabwe, and electronic results transmission in Nigeria, among others – other countries have become increasingly wary of applying it for voting processes. Ireland put the use of electronic voting machines on hold months before their planned use in nationwide elections in 2004[19] and officially dropped the plan in 2009.[20] After Finland piloted the use of electronic voting machines (EVM) in three municipalities (with traditional paper balloting also allowed),[21] the results were later annulled by the Supreme Administrative Court.[22] Subsequently, the Finnish government decided to stop using this technology.

DRAFT

Following Germany's 2005 parliamentary (*Bundestag*) elections, the Federal Constitutional Court ruled on two complaints about the use of computerized voting machines. Alleging insufficient transparency, the complainants sought to invalidate the elections and to repeat them with paper voting slips and ballot boxes. The Court found that the EVMs used were insufficiently transparent to the public; votes were recorded only on an electronic storage medium, so voters could not verify that their choices were recorded correctly and could only see that the machines had registered a ballot. The Court did not dissolve the *Bundestag* with its decision but declared the use of electronic voting machines unconstitutional if it is not possible

---

and Democratic Values, 73 Fordham L. Rev. p. 1719.
https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4064&context=flr

[16] The Rationale for E-voting in Brazil | National Democratic Institute (ndi.org)

[17] A Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment (nist.gov)

[18] India's electoral democracy: How EVMs curb electoral fraud (brookings.edu)

[19] Commission on Electronic Voting. (2004, December). First Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System.
https://opac.oireachtas.ie/Data/Library3/Library2/DL049949.pdf

[20] RTÉ. (2009, April 23). Electronic voting system to be scrapped. https://www.rte.ie/news/2009/0423/evoting.html

[21] Vaalit Val, Department for Democracy and Public Law, Ministry of Justice. Electronic voting in Finland.
https://vaalit.fi/en/electronic-voting1

[22] European Digital Rights (EDRi). (2009, April 22). Finnish e-voting results annulled by the Supreme Administrative Court.
https://edri.org/our-work/edri-gramnumber7-8evoting-annuled-finland/

for voters to reliably examine, without specialist technical knowledge, that the machine correctly recorded their vote.[23]

Technology reversals in elections have largely been predicated on security concerns. Large-scale attacks targeting foreign public and private institutions have become more common since the early 2000s.[24] Instances of Chinese hackers infiltrating U.S. networks to acquire national security information or intellectual property have been documented since 2003.[25] In 2007, Estonia's government and banking sectors experienced their first major international cyber attack – a large-scale Distributed Denial of Service (DDoS) that was attributed to the Russian Federation.[26] Similar attacks followed in Georgia and Kyrgyzstan and, later, in Bulgaria.[27] In 2014, electoral technology was spotlighted in the cybersecurity debate when Russian hackers attacked the Ukrainian Central Election Commission's website and published false results declaring that an ultra-right candidate had won the election. The attack intended to undermine Ukrainians' trust in elections,[28] and it marked the onset of broader efforts to diminish public confidence in democratic processes.

Attacks on the U.S. election infrastructure during the 2016 presidential election further highlighted the severity of the threat. In 2020, during the COVID-19 pandemic, many U.S. states expanded absentee and vote-by-mail voting, temporarily introducing universal vote-by-mail, online voter registration and online applications for absentee ballots. Online voter portals in several states crashed close to absentee request cut-off dates, requiring that request deadlines be extended.[29] It remains unclear whether this was the result of a benign issue such as strong demand by legitimate requests overloading the sites, or whether this was the result of malicious denial of services attacks. In 2021, the German election administration was also targeted by cyber attacks.[30] The same week the German election administration detected attempted cyber attacks, the Russian election commission CEC also reported attacks during its three-day voting period.[31]

DRAFT

---

[23] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

[24] Significant Cyber Incidents (n.a.). Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/210901_Significant_Cyber_Incidents.pdf?iZAairy6vNXrSEp9cFC_TCaB0IxnkE3D. Accessed on 09/03/2021.

[25] Ibid.

[26] Ottis, R. (2018) Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defense Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[27] Kozlowski, A. (2014). Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal. 3(4), 237-245 ; http://connections-qj.org/article/blending-new-generation-warfare-and-soft-power-hybrid-dimensions-russia-bulgaria-relations; https://www.president.bg/news3428/interview-of-president-plevneliev-for-the-bbc.html&lang=en); https://www.bbc.com/news/world-europe-37867591

[28] For a dissection of this development, see Martin-Rozumilowicz and Chanussot (2019).

[29] https://urbanmilwaukee.com/2020/04/02/absentee-ballot-deadlines-extended-election-not-delayed-by-federal-judge/

[30] https://www.securityweek.com/german-election-authority-confirms-likely-cyber-attack

[31] https://www.easternherald.com/2021/09/20/cyber-attacks-russia-elections/

While some countries have stepped back from automating the voting process because of security and transparency concerns, the world has more uniformly moved toward election technology to digitize voter registers and transmit and aggregate election results. There are multiple sources of policy, principle, and practice in cybersecurity in elections, including international, regional, and domestic standards and laws; good practice publications from practitioner organizations; cybersecurity instruments and frameworks; election observer guidelines; and academic literature. The content that follows in this brief literature review offers an introduction to these sources, drawing on and updating text initially published in the 2018 IFES paper Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies.[32]

A. International, Regional and Domestic Standards for Cybersecurity in Elections

International standards for cybersecurity, transparency, open data and privacy stem from – and must adhere to – fundamental political rights established by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). These standards include the United Nations (UN) General Assembly Guidelines for the Regulation of Computerized Data Files;[33] the European Parliament's General Data Protection Regulation (GDPR);[34] the United Nations Privacy and Data Protection Principles; and the Open Government Declaration, which 75 countries signed in 2011, committing to advance transparency and openness within government.[35]

DRAFT

The Open Government Declaration includes a provision for increasing access to and use of new technology in order to make government practices transparent, secure online spaces and platforms, as well as to provide "alternative mechanisms of civic engagement."[36] The declaration also provides standards that require signatories to "increase the availability of information about governmental activities." This includes open access to government data so that information can be easily found and used. The importance of open data is enshrined in the declaration: "We recognize the importance of open standards to promote civil society access to public data, as well as to facilitate the interoperability of government information systems."[37] These standards will be essential when implementing voting and counting technology, where individual information must be securely and transparently stored and checked to ensure the validity of both the voters and the votes

[32] Katherine Ellena, et al., Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies, IFES, (Arlington, VA: 2018)

[33] United Nations General Assembly, Guidelines for the Regulation of Computerized Data Files, 14 December 1990, res. 45/95, http://www.refworld.org/pdfid/3ddcafaac.pdf.

[34] Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

[35] Open Government Partnership, Open Government Declaration, 2011, https://www.opengovpartnership.org/open-government-declaration. Since joining in 2011, Hungary and Turkey withdrew their participation. Azerbaijan's status is inactive since 2015.

[36] Ibid.

[37] Ibid.

Beyond these instruments, international organizations and governing bodies are increasingly establishing international standards on the conduct of elections in which any election-related data is stored digitally. Although not the first forum to establish guidelines on data management, recognized international standards are summarized in the United Nations (UN) General Assembly Guidelines for the Regulation of Computerized Data Files.[38] Adopted by the General Assembly in 1990, these guidelines provide broad principles of data management that place responsibility for data on those persons who collect it, specifically requiring that data collectors be responsible for ensuring that the data is accurate, transparently and lawfully collected, properly restricted to avoid discrimination, securely stored, and lawfully disseminated.[39] The UN guidelines do not provide specific technical requirements to ensure that these principles are met, and the guidelines apply only to "governmental international organizations."[40] These guidelines define the principle of security as taking appropriate action to "protect the files against natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses."[41] Though the guidelines do not explicitly mention election technology, they have implications for electronic data management in electoral processes and outline protections that should apply to the full range of stakeholders involved in the electoral process – voters, candidates, election officials, among others – whose data may be collected.

There are additional standards for the introduction of technology in voting or vote-counting processes specifically. Most notably, the Council of Europe's 2017 e-voting standards place specific responsibility on EMBs for the "availability, reliability, usability and security of the e-voting system."[42] The Council of Europe also maintains a set of non-binding standards for e-voting that cover the application of general principles, such as universal suffrage and accountability, to e-voting technology. Universal suffrage requires that voting interfaces are easy to use and understand for all voters, for example, and accountability requires that the system be open to audits and that EMBs maintain responsibility for ensuring compliance with security requirements "even in the case of failures and attacks."[43]

Some countries establish their own voluntary standards or legislation. For example, the U.S. Electoral Assistance Commission maintains a set of voluntary guidelines to help election authorities test whether their systems meet certain functionality, accessibility and security standards. Many U.S. jurisdictions have adopted these standards as obligatory.[44] Certification of election technologies has also been captured in the Council of Europe's guidelines for certifying

DRAFT

---

[38] United Nations General Assembly, Guidelines for the Regulation of Computerized Data Files, 14 December 1990, res. 45/95. http://www.refworld.org/pdfid/3ddcafaac.pdf

[39] Ibid.

[40] Ibid., sec. B.

[41] United Nations General Assembly, Guidelines for the Regulation of Computerized Data Files, sec. A(7).

[42] Council of Europe, CM-Rec (2017)5, 17 June 2017, Appendix I, sec. VIII. This is a revision of the 2004 standards, which were the first of their kind.

[43] Council of Europe, CM-Rec. (2017)5, Appendix I, sec. VIII.

[44] "Voluntary Voting System Guidelines," Voting Equipment, U.S. Election Assistance Commission (EAC), https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

e-voting systems, which focused on selecting certification bodies, renewing certification, and conducting cost-benefit analyses.[45]

The field of cybersecurity in elections is still emerging, both in national legislation and in international jurisprudence and standards. Apart from the Council of Europe's 2006 Cybercrime Convention (Budapest Convention), there are no other binding international instruments at present that directly tackle prevention of and punishment for cyberattacks.[46] Countries often have general security regulations that do not cover all cybersecurity-related issues, or they are scattered in multiple pieces of legislation and government regulations, some of which may be outdated. A coherent legal framework for cybersecurity is important. For example, Ukraine passed a Law on Cybersecurity, which took effect in May 2018, in response to its dire need to systematically handle cyber attacks, such as the (Not)Petya malware attacks of June 2017.[47]

The privacy of the individuals whose data is collected is another important element of data management that has become particularly prominent with the recent passage of the European Union's (EU) General Data Protection Regulation (GDPR),[48] which went into effect in May 2018. This regulation governs personal data of EU residents that companies and organizations collect, store or process, and requires more openness about what data they have and who they share it with.[49] The UN has adopted various general resolutions on data privacy[50] to ensure the privacy of individuals or groups whose data is collected. Collectively, these principles aim to ensure transparency in the collection of data to protect the use of this data and offer the opportunity to determine whether information is accurate and non-discriminatory.

DRAFT

B. Good Practice Guidelines for Implementing Election Technology

In addition to international, regional, and domestic standards, a substantial number of intergovernmental and international non-governmental organizations, including the Council of Europe, European Commission, IFES, International IDEA, the National Democratic Institute (NDI), and the Organization for Security and Co-operation in Europe's Office for Democratic Institutions and Human Rights (OSCE/ODIHR), among others, have contributed guidelines and handbooks on election technologies to this conversation. The Declaration of Principles (DoP) community, which brings together 55 international organizations around a common set of observation criteria, has developed the forthcoming technical document General principles and

[45] Council of Europe, Certification of e-voting systems, 2011.

[46] https://www.coe.int/web/cybercrime/the-budapest-convention

[47] The original ransomware attack known as "Petya" held hostage data from several companies and demanded a ransom to release it. A number of cybersecurity analysts maintain that the newer versions were instead aimed at causing damage. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

[48] Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

[49] European Commission website, "What does the General Data Protection Regulation (GDPR) govern?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

[50] G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989). See also General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014, as well as Human Rights Council resolutions 28/16 of 26 March 2015 on the right to privacy in the digital age and 32/13 of 1 July 2016 on the promotion, protection and enjoyment of human rights on the Internet.

guidelines related to ICT and elections. The DoP publication seeks to highlight the responsibilities of various stakeholders in the use of technology in elections, and emphasizes that "E-ICT systems should follow the key principles for democratic elections, including granting the integrity, secrecy, universality and equality of the vote, transparency, accountability, digital security and public confidence (trust)."[51]

Several recent practitioner publications explicitly connect cybersecurity and elections. For example, in February 2018, the Center for Internet Security (CIS) published "A Handbook for Elections Infrastructure Security," which identifies election system risks and good practices that county or state election administrators could implement to mitigate those risks.[52] The Global Cyberalliance used this handbook to create the GCA Cybersecurity Toolkit for Elections, which provides free cybersecurity tools for election officials.[53] CIS also released a "Cybersecurity Supply Chain Risks in Election Technology" guide in 2021."[54]

The Harvard Kennedy School's Belfer Center developed a "State and Local Election Cyber-Security Playbook" for U.S. election officials but that can also be used in wider contexts.[55] This publication offers a myriad of recommendations organized by various topics and using the five-step functional approach developed by the National Institute of Standards and Technology (NIST). The Brennan Center for Justice at New York University has published "Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials' as well as an accompanying security planning checklist, which focuses on preventing and addressing technological failures, errors, and attack.[56] In July 2018, the EU Cooperation Group[57] published a "Compendium on Cyber Security of Election Technology" that aims to systemize the cyber concerns and threats across the European continent and offers myriad experiences accumulated from EU member states' elections in case studies.[58] The International Institute for Democracy and Electoral Assistance (International IDEA) has also released a guide focusing on the role of interagency collaboration in protecting elections against digital threats. It contains 20 country case studies on improvements to election cybersecurity, ongoing risks to cybersecurity, and each country's progress towards interagency collaboration.[59]

DRAFT

[51] The Declaration of Principles (DoP) for International Election Observation and the Code of Conduct for International Election Observers is available at: https://www.ndi.org/DoP See also DoP General Principles and Guidelines Related to ICT and Elections, forthcoming.

[52] https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

[53] Global Cybersecurity Alliance. (2019). The GCA Cybersecurity Toolkit for Elections. https://gcatoolkit.org/elections/

[54] https://learn.cisecurity.org/Managing-Cybersecurity-Supply-Chain-Risks-in-Election-Technology

[55] Harvard Kennedy School's Belfer Center, Defending Digital Democracy Project (D3), The State and Local Election Cyber-Security Playbook, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[56] Cortes, E. Ramachandran, G. Howard, L., Norden, L. (2019). Preparing for Cyberattacks and Technical Failures A Guide for Election Officials. Brennan Center for Justice at New York University School of Law. https://www.brennancenter.org/our-work/policy-solutions/preparing-cyberattacks-and-technical-failures-guide-election-officials

[57] Comprising experts from the EU member states, the European Commission and ENISA.

[58] EU NIS Cooperation Group, Compendium on Cyber Security of Election Technology, July 2018, https://www.ria.ee/public/Cyber_security_of_Election_Technology.pdf

C. Cybersecurity Instruments and Frameworks

Several high-level policy institutes have developed cybersecurity frameworks to systematically address cyber-threats and vulnerabilities in any complex system. These organizations include the National Institute of Standards and Technology (NIST),[60] the information systems non-profit ISACA,[61] the International Organization for Standardization (ISO),[62] and the U.S. Computer Emergency Readiness Team (US-CERT).[63] In the absence of comprehensive election-specific cybersecurity standards, these general frameworks may be useful for EMBs. Cyber-security frameworks are typically organized using a functional approach (i.e., breaking down processes into specific functions). NIST, together with US-CERT, identified a functional approach in its framework in five steps that is now widely used within the cybersecurity community: identify; protect; detect; respond; and recover.

TNIST also runs the Computer Security Resource Center, which keeps its 800-series publications (resources focused on cybersecurity) in one searchable archive. These publications range from targeted security recommendations, such as email protection or message authentication code algorithms, to good practices for employees and general frameworks. ISACA provides a framework for information systems security audits[64] and a framework for balancing the risks and benefits of IT.[65] The latter is based on five principles: 1) meeting stakeholder needs; 2) covering the enterprise end-to-end; 3) applying a single, integrated framework; 4) enabling a holistic approach; and 5) separating governance from management.[66]

DRAFT

The EU Agency for Network and Information Security (ENISA) and ISO have also identified critical cyberthreats. ISO's cybersecurity guidelines (produced through a joint committee with the International Electrotechnical Commission) includes a list of more than 50 threats, and ENISA publishes an annual "Threat Landscape" report identifying the top 15 cyberthreats that year.[67] While some are more directly relevant to EMBs than others, all could be used to undermine the security and legitimacy of the electoral process. ENISA identified threats as diverse as information leakage, such as in the 2017 French elections, cyber espionage, such as the Russian involvement in the 2016 U.S. elections, ransomware, and insider threats.[68] The

---

[59] Van der Staak, S. Wolf, P. (2019). Cybersecurity in Elections Models of Interagency Collaboration. International Institute for Democracy and Electoral Assistance. https://www.idea.int/publications/catalogue/cybersecurity-in-elections

[60] National Institute of Standards and Technology, https://www.nist.gov/.

[61] ISACA, https://www.isaca.org/Pages/default.aspx?gclsrc=aw.ds.

[62] International Organization for Standardization, https://www.iso.org/home.html.

[63] US-CERT, https://www.us-cert.gov/.

[64] Shemlse Gebremedhin Kassa, "Information Systems Security Audit: An Ontological Framework," ISACA Journal vol. 5, 2016, https://www.isaca.org/Journal/archives/2016/volume-5/Pages/information-systems-security-audit.aspx.

[65] "COBIT," ISACA, http://www.isaca.org/cobit/pages/default.aspx.

[66] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, Executive Summary.

[67] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27005:2011, 2011; European Union Agency for Network and Information Security, ENISA Threat Landscape Report 2017, 2018.

[68] ENISA, ENISA Threat Landscape Report 2017, 79-87.

diverse landscape of threats from inside and outside an organization demonstrate the need for comprehensive and systematic cybersecurity protection.

NIST has also recently released a draft Cybersecurity Framework Election Infrastructure Profile, which could provide EMBs with additional guidance specifically on election security.[69] The profile, which was released for public comment in 2021, focuses on reducing cybersecurity risks to election infrastructure and leverages the NIST Cybersecurity Framework to inform good practices. Given that jurisdictions in the United States vary in the technologies they use for elections, NIST highlights that the profile is designed to aid election officials to mitigate risks regardless of the system a jurisdiction uses.[70] The various risk management frameworks are discussed in greater detail in subsequent sections.

D. Election Observer Guidelines

As well as introducing new operational and security considerations, emerging election technology has also changed the observation of elections. Several election observer groups and networks have promulgated guidelines for the observation of elections in the modern, technology-driven context (for example, the OSCE/ODIHR Handbook for the Observation of New Voting Technologies and Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions. [71] These documents provide observation teams with election technology standards and good practice guidelines.

The consensus among these groups favors more technical skills for core teams, longer and earlier missions, and closer observation of election technology – including during the development of specifications and the procurement stage. The Carter Center's Handbook on Observing Electronic Voting recommends having at least two members of a core observer team with technical skills, ideally with a combination of electoral experience and technological and/or computer science skills. These "e-voting experts" should have five to ten years of relevant experience.[72] Core team members without a technical background need additional training to evaluate the technical aspects of the electoral process. The Organization of American States (OAS) recommends that a "core group" of technical staff and specialists, along with long-term observers, conduct an analysis of the technology to be used in the upcoming elections. The results should be used to determine the training needed for short-term observers.[73]

DRAFT

---

[69] Brady, M. Howell, G. Sames, C., Schneider, M. Snyder, J. Weitzel, D. Franklin, G. (2021). Cybersecurity Framework Election Infrastructure Profile. National Institute of Standards and Technology, U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/nistir/8310/draft

[70] National Institute of Standards and Technology, U.S. Department of Commerce. (2021, March 29). To Help Protect Our Elections, NIST Offers Specific Cybersecurity Guidelines. https://www.nist.gov/news-events/news/2021/03/help-protect-our-elections-nist-offers-specific-cybersecurity-guidelines

[71] See, OSCE/ODIHR Handbook for the Observation of New Voting Technologies (https://www.osce.org/odihr/elections/new_voting_technologies) and OAS Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions (https://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf).

[72] The Carter Center, Observing Electronic Voting, (Georgia: 2012), 5.

[73] Gustavo Aldana, et al., Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions, OAS, 8.

New technology requires extra preparation on the part of election observation missions (EOMs). According to The Carter Center, EOMs should start as early as possible, typically four to six months before an election, and stay until any dispute resolution has finished.[74] NDI recommends observer involvement at every stage of the technological adoption process, including developing specifications for hardware and software, testing the technology, and reviewing training manuals and attending training sessions for EMB employees.[75] The Carter Center, ODIHR and the OAS provide a questionnaire for observers monitoring new election technology; the OSCE has a checklist of questions in their Handbook for the Observation of New Voting Technologies.[76] This demonstrates that observer groups are adapting to the new requirements that election technology presents, although funding and resources can be a challenge in supporting longer-term and more technical observation.

E. Academic literature

New election~~voting~~ technologies, and the vulnerabilities these technologies can introduce to election processes have been a central focus of election cybersecurity research by academia. This research has especially concentrated on evaluating various forms of electronic voting: in-person electronic voting via direct-recording electronic voting machines (DREs); remote, paperless voting, including internet voting; and certain applications of blockchain-based voting.

DRE machines provide an electronic alternative to paper ballots. While some DRE machines have the capacity to record votes on paper, others operate using entirely paperless systems and consequently lack a voter-verifiable paper audit trail (VVPAT).[77] This latter subset has been the focus of extensive scholarly research, which has identified critical vulnerabilities in such systems that would permit malicious actors to manipulate electoral results.[78]

DRAFT

In the United States, Feldman et al. demonstrate that malicious actors could gain access to the Diebold AccuVote-TS machine, a DRE machine that was widely used in the 2006 United States general election.[79] Upon gaining access by installing malicious code on a machine, an attacker would be able to steal votes as well as ensure that a voting machine virus spread to other machines.[80] Tests conducted by researchers on DRE machine systems in California and Ohio

---

[74] The Carter Center, Observing Electronic Voting, 2012, 6-7.

[75] Vladimir Pran and Patrick Merloe, Monitoring Electronic Technologies in Electoral Processes, NDI, (Washington, DC: 2007), 35-41.

[76] The Carter Center, Observing Electronic Voting, 2012, 41-65; Aldana, et al., Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions, 33-35; OSCE, Handbook for the Observation of New voting Technologies, (Warsaw, Poland: 2013), 70-71.

[77] Gambhir, R. K., & Karsten, J. (2019). Why Paper Is Considered State-of-the-Art Voting Technology. Brookings Cybersecurity and Election Interference. Norden, L., Cordova McCadney, A. (2019, March 9). Voting Machines at Risk: Where We Stand Today. Brennan Center for Justice at New York University School of Law. Feldman, A., Halderman, J., Felten, E. (2007). Security Analysis of the Diebold AccuVote-TS Voting Machine. Security Analysis of the Diebold AccuVote-TS Voting Machine. In Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07). https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html

[78] Ibid. Gambhir, R. K., & Karsten, J. (2019). Why Paper Is Considered State-of-the-Art Voting Technology. Brookings Cybersecurity and Election Interference

[79] Feldman, A., Halderman, J., Felten, E. (2007). Security Analysis of the Diebold AccuVote-TS Voting Machine. Security Analysis of the Diebold AccuVote-TS Voting Machine.

yielded similar results.[81] In India, a test of the country's electronic voting machines—nearly 1.4 million of which were in use for the 2009 Indian parliamentary elections—also demonstrated that the machines were vulnerable to attacks that would be able to alter election results.[82] In the Netherlands, a review of the country's DRE machine, used by 90% of Dutch voters, revealed that if a malicious actor were to gain brief access to the device prior to the election, the actor would acquire nearly undetectable control of the results.[83] The results of this review contributed to the retirement of the NEDAP ES3B in the Netherlands and a return to paper voting.[84]

Many evaluations of paperless DRE technology were concentrated in the early- and mid- 2000s, when the adoption of DRE machine technology increased, particularly in the United States.[85] Given the high cost of replacing voting systems, DRE machines may be paired with VVPAT sub-systems which creates a paper record of a vote and can be used to conduct risk-limiting audits or recount elections.[86] This solution can ensure that DRE machines are auditable and help officials identify vote-stealing attacks.[87] Park et. al note that by incorporating, for example, a paper record of evidence into the voting process, an election system can be auditable. An election that is both auditable and audited satisfies the conditions to be considered an evidence-based election.[88] VVPATS and audits, however, are not a complete solution to the risks accompanying DRE machines. These measures would not be able to prevent disruptions in the form of denial-of-service attacks, which could disable voting machines on Election Day.[89]

Broad consensus exists on the risks DRE machines lacking a VVPAT sub-systems pose to election results;[90] conversely, internet voting technology continues to be embraced and piloted as

DRAFT

---

[80] Ibid.

[81] Balzarotti, D., Banks, G., Cova, M ., Felmetsger, V., Kemmerer, R., Robertson, W., Valeur, F., Vigna, G. (2010). An Experience in Testing the Security of Real-World Electronic Voting Systems. IEEE Transactions on Software Engineering, vol. 36, no. 4, pp. 453-473. https://ieeexplore.ieee.org/document/5210119.

[82] Wolchok, S., Wustrow, E., Halderman, J., Prasad, H., Kankipati, A., Sakhamuri, S., Yagati, V., Gonggrijp, R. (2010, October). Security analysis of India's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 1-14).

[83] Gonggrijp, R., & Hengeveld, W. J. (2007, August). Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective. In Proceedings of the USENIX workshop on accurate electronic voting technology (pp. 1-1).

[84] National Democratic Institute. Re-evaluation of the Use of Electronic Voting in the Netherlands. https://www.ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands

[85] MIT Election Data + Science Lab. Voting Technology. https://electionlab.mit.edu/research/voting-technology

[86] Ibid. Harvard Kennedy School's Belfer Center, Defending Digital Democracy Project (D3), The State and Local Election Cyber-Security Playbook, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook Norden, L., Cordova McCadney, A. (2019, March 9). Voting Machines at Risk: Where We Stand Today. Brennan Center for Justice at New York University School of Law.

[87] Norden, L., Cordova McCadney, A. (2019, March 9). Voting Machines at Risk: Where We Stand Today. Brennan Center for Justice at New York University School of Law. Feldman, A., Halderman, J., Felten, E. (2007). Security Analysis of the Diebold AccuVote-TS Voting Machine. Security Analysis of the Diebold AccuVote-TS Voting Machine.

[88] Park, S., Specter, M., Narula, N., Rivest, L R. (2020, December 4).Going from bad to worse: from Internet voting to blockchain voting. Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyaa025, https://doi.org/10.1093/cybsec/tyaa025

[89] Feldman, A., Halderman, J., Felten, E. (2007). Security Analysis of the Diebold AccuVote-TS Voting Machine. Security Analysis of the Diebold AccuVote-TS Voting Machine. p. 14

election officials globally consider the implementation of internet voting technology.[91] However, tests by researchers on existing and pilot internet voting systems have revealed vulnerabilities that, similar to those outlined in studies of paperless DRE machines, would allow actors to control and manipulate election results. A 2020 study of Switzerland's pilot internet voting system, an earlier version of which has been used in certain Swiss cantons, uncovered that the system contained vulnerabilities that would allow for the construction of proofs of accurate election outcomes even if the results were manipulated.[92] Similarly, experimental attacks of a reproduction of Estonia's voting system,[93] the first in the world that used internet voting at the national level, and of a Washington D.C. online voting pilot tool[94] both revealed possible vulnerabilities that would allow attackers to alter election results.

Given existing vulnerabilities with certain remote voting systems, blockchain technology has emerged as a possible solution to ensure greater security of remote voting. Researchers open to the use of this technology highlight blockchains' ability to create "cryptographically secure voting records" and ensure that votes are recorded but are unable to be manipulated by attackers without being detected.[95] Moreover, researchers cite the possibility of blockchain technology to replace paper-based election systems and outline the cost-savings and beneficial impacts to transparency and participation it could provide.[96]

The benefits of blockchain technology to support remote voting, however, are not universally accepted. Research on the use of blockchain technology highlights its existing limitations,[97] while other work directly opposes its implementation and warns that certain existing risks to remote voting systems, such as the risks associated with internet voting, would persist in the case of internet voting with additional security supported by blockchain technology. Moreover, the research raises the possibility of blockchain-based voting introducing additional security risks.[98] A reverse engineering of Voatz, a mobile app used in West Virginia during the 2018 United States midterm elections, revealed vulnerabilities that would allow adversaries to "alter, stop, or expose a user's vote."[99] A description of Voatz' security model is not publicly available,

DRAFT

---

[90] Gambhir, R. K., & Karsten, J. (2019). Why Paper Is Considered State-of-the-Art Voting Technology. Brookings Cybersecurity and Election Interference.

[91] Park, S., Specter, M., Narula, N., Rivest, L R. (2020, December 4). Going from bad to worse: from Internet voting to blockchain voting. p. 2

[92] Haines, T., Lewis, S. J., Pereira, O., Teague, V. (2020) How not to prove your election outcome. 2020 IEEE Symposium on Security and Privacy (SP), pp. 644-660, doi: 10.1109/SP40000.2020.00048.

[93] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J. Security analysis of the Estonian internet voting system. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages 703–715. ACM, 2014.

[94] Wolchok S., Wustrow E., Isabel D., Halderman J.A. (2012) Attacking the Washington, D.C. Internet Voting System. In: Keromytis A.D. (eds) Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, vol 7397. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32946-3_10

[95] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4). p.3

[96] Ibid.

[97] Ibid.

[98] Park, S., Specter, M., Narula, N., Rivest, L R. (2020, December 4).Going from bad to worse: from Internet voting to blockchain voting.

but the app's owner claims blockchain is one of multiple components used to safeguard the application.[100] Additionally, tests conducted on an internet voting system leveraging blockchain technology for residents of Moscow discovered vulnerabilities in the system and allowed researchers to launch two successful attacks on the system's encryption scheme.[101] Further exploration may be required to understand the capability of this technology to adequately safeguard remote voting systems.

III. Integrating a risk-based lens to understand election cybersecurity

As information technology environments have developed and evolved, becoming more complex over time, the field of cybersecurity was born out of necessity. As the threats that take advantage of this complex environment have become more sophisticated, the cybersecurity field has become professionalized over time, evolving past the stage of simple checklists that indicate requirements for IT generalists to implement; modern frameworks instead characterize cyber threat detection and mitigation as a continuous process of risk management with industry standard practices to be performed by specialists.

Risk management is a discipline in and of itself and there are several standard risk management frameworks. The most commonly used are: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, which is specific to information technology contexts;[102] the International Organization for Standardization (ISO) 31000 series, which is a generic risk management framework and can be applied in conjunction with ISO 27001 IT controls.[103] The European Union Agency for Cybersecurity (ENISA) Risk Management/Risk Assessment (RM/RA) framework is also a comprehensive source of risk management standards and security controls.[104] Each of these frameworks – and the associated sets of security and privacy controls (discussed below) – have been designed based on specific national requirements, policies and laws. For example, the NIST framework was designed based on the U.S. context, while the ENISA framework is responsive to the European context. Governments and industry have widely adopted and typically follow them in the absence of a national framework. However, adherence to and implementation of these frameworks is often limited by strained resources, competing priorities and lack of cybersecurity advocacy.

DRAFT

---

[99] Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 1535-1553).

[100] Ibid.

[101] Gaudry, P., & Golovnev, A. (2020, February). Breaking the encryption scheme of the Moscow internet voting system. In International Conference on Financial Cryptography and Data Security (pp. 32-49). Springer, Cham.

[102] NIST SP 800-37 is specific to the information technology concepts and is available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[103] The ISO 31000 framework is a general risk management framework that can be applied in various contexts, not just IT. Available at: https://www.iso.org/iso-31000-risk-management.html; the ISO 27001 standard establishes information technology security controls to be applied within the larger risk management framework

[104] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-processintegration/the-enisa-rm-ra-framework

The purpose of this section is not to endorse any specific framework and associated controls, but rather to introduce risk management and security control mechanisms generally, and to discuss cybersecurity as applied across the election cycle.

The risk management process, as applied to electronically processed information, requires cybersecurity specialists to: 1) identify information and technology assets; 2) categorize both in terms of the impact of a potential loss or compromise; 3) assign and apply security and privacy controls based on prior categorization; 4) continuously evaluate the efficacy of those controls; and 5) feed information back into the process to continuously and proactively improve the controls.[105] While the premise is simple, operationalizing this process is not a trivial task. Security controls are descriptions of discrete actions that can be taken to help mitigate risks. [106] Different frameworks separate controls into various aggregations, but the following three categories are useful for this discussion:[107] management controls, operational controls and technical controls. *Management controls* use planning and assessment methods to help control risk (e.g., programmatic guidelines and policies, assessments to understand efficacy of budget planning and other enterprise-wide policies and protections that are scoped and executed administratively). *Operational controls* address the policies and protections that contribute to the secure operation of information systems throughout the lifecycle of a system, and are implemented through people executing processes (e.g., mandating specific change management steps, contingency planning or awareness training). *Technical controls* are implemented through the use of technology (e.g., encryption of data at rest and during transmission, automated monitoring and alarming and the use of verifiable security tokens to prove identity).

DRAFT

The controls themselves are put into practice at (and pertain to) various levels, ranging from the abstract cybersecurity program level (managing and implementing organized cybersecurity across an enterprise) down to physical hardware and software controls that implement specific security mechanisms. In addition to the program level, other commonly used categories include the site level (e.g., within a facility or across a location), the network level, the environment level (i.e., aggregated systems that are part of a cohesive whole, such as the server environment or wireless access environment), and the host level (referring to a single computer system).

Controls, however, are not the only way to manage cybersecurity risk. Risk can also be transferred via mechanisms such as insurance, through contractual relationships, or between agencies or departments due to division of responsibilities. Within the election space, such risk transference mechanisms may not be easily utilized nor appropriate, depending on, among

---

[105] This is a simplification for understanding and brevity of the process described in depth within NIST, ISO, ENISA and other risk management frameworks

[106] NIST SP 800-53 Rev. 5 defines a core set of security and privacy controls that operationalize the framework elucidated in 800-37. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[107] NIST SP 800-53 divides controls into 20 “control families.” for security and privacy while ISO27001 utilizes 14 “control sets.” The three categories presented here are a general consolidation for the purpose of the present discussion. Another set of commonly utilized controls comes from the Center for Internet Security (CIS) and is divided among 18 categories, available at: https://www.cisecurity.org/controls/cis-controls-list/

other things, the type of EMB institutional arrangement or national policies and legal frameworks. In cases where risk cannot be mitigated or transferred, it can be accepted to facilitate operations. If risk is deemed too great, the information system or technology can be rejected for use. If the decision is made to adopt the system or technology despite the risks, the system is considered authorized. In this case, it should be managed throughout its lifecycle, from procurement through disposal, within the defined risk management framework.[108] Controls also involve defining the mechanisms of response during cybersecurity incidents.[109] Planning for response and post-event resiliency is an integral part of managing cybersecurity risk.

On the whole, a well-defined cybersecurity risk management process puts in place a holistic mechanism to understand and manage the risk of operating information systems and electronic networks. Executing the process identifies risks that are either mitigated, transferred (in contexts where appropriate and if circumstances allow), or in some cases accepted. This accepted risk is then identified and tracked within a risk register. Risk registers are continuously updated as new risks are identified and others retired (which takes place when controls are developed and applied to mitigate known risks, or when risks are eliminated).[110]

Effective cybersecurity requires buy-in at the executive levels of an organization, as well as implementation throughout all levels of an organization. In the context of elections, EMB leadership is often risk-averse when it comes to modern technologies. The prospect of adopting new technologies to replace or complement traditional mechanisms used in electoral processes is daunting to many EMBs, as they consistently face limited time, resources, and capacity. As noted in the IFES paper "Raising Trust in Electoral Technology," "Not only do many [EMBs] struggle to establish appropriate procedures and training for the new technologies, they also unfortunately neglect to maintain their traditional mechanisms. The compounding nature of these two factors create immense risks for their election."[111]

DRAFT

As such, the threat environment is likely to outpace an EMB's technology adoption; simultaneously, user practices consistently evolve ahead of new policy adoption, creating areas of unaccounted risk. Given this, the threat environment should drive EMB management to seek and advocate for necessary increases in resources, training and procurement, in addition to encouraging them to install policies to reduce cybersecurity risks. In modern organizations, cyber risk management is a matter of strategic planning and a key responsibility of executives, not simply a matter for IT departments functioning in vacuums to address.

---

[108] Not discussed here are the granular actions that operationalize the high-level process. This includes the use of specific plans, sometimes referred to as "information system security plans," that help organize the implementation of controls on and across discrete information systems and networks.

[109] The particulars of which are also not defined nor developed within the present discussion.

[110] It should be noted that often applied security controls can only sufficiently mitigate a portion of the risk present with the operation of any specific information asset or associated process, the "left over risk" that is uncontrolled is characterized as "residual risk" that must be recognized and deemed acceptable or rejected. This residual risk is also defined and tracked within the risk register.

[111] Erben, Peter. (2017). IFES. Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches. https://www.ifes.org/sites/default/files/ifes_erben_raising_trust_in_electoral_technology_innovation_aided_by_traditional_approaches_d8_sep_2017.pdf.

Globally, there have been only limited efforts taken by EMBs to systematically mitigate cyber-related risks. There is, however, an increasingly explicit understanding that actors interacting with a system bear responsibility for, and must be involved in, its cybersecurity. Previously, election administrators understood their role to be that of a civil servant administering a bureaucratic process from behind the curtain; however, the last decade has made them front-line workers and first responders addressing critical situations that impact national security. To keep up with the evolution of the threat environment and evolve their cybersecurity postures accordingly, EMBs and other institutions must first assess and understand their current cybersecurity capacity strengths and gaps.

There are several applicable cybersecurity maturity models, which institutions ~~; institutions can~~ can use ~~these models~~ to assess their cybersecurity capacity and identify and define their current position, before identifying their desired future maturity state. These maturity models help organizations locate their baseline cybersecurity activity on a scale. For example, *level 0* corresponds to the absence of cybersecurity activities and practices, while *level 1* indicates that some practices and capabilities are in place, albeit *ad hoc* in nature. *Level 2* indicates that cybersecurity practices are documented and there is institutionalized support and resources for those documented processes. *Level 2* maturity may also mean that cybersecurity, overall, is still reactive within the organization, while *level 3* indicates a more adaptable and proactive posture.[112] Maturity indicators can not only help to understand the programmatic and managerial characteristics of an organization's cybersecurity position, but they are also necessary to evaluate the cybersecurity workforce. The U.S., for example, has developed the National Initiative for Cybersecurity Education (NICE) Framework. The NICE framework defines seven high-level categories of common cybersecurity functions and 52 separate work roles. Each work role has defined skills and knowledge associated with it, which help guide measures of maturity to determine the baseline skillset required of persons filling those roles.[113]

DRAFT

There are obvious challenges preventing EMBs from embracing and implementing comprehensive risk management-based cybersecurity programs across the activities that fall under their responsibility. These include the unique EMB institutional arrangements in various countries across various contexts, limited resources and competing priorities, immature national and local cybersecurity mechanisms, a lack of cybersecurity education, and a range of operational and technical impediments. However, introducing the risk-management approach to defining, understanding, and discussing these challenges can help clarify steps EMBs can take toward strengthening their cybersecurity postures. There are several countries that already have policies in place requiring EMBs to implement the risk management approach for cybersecurity via the frameworks referenced above, however uptake is far from institutionalized and substantial progress remains to be made.[114]

---

[112] For a broad overview of the concept of maturity models, along with a U.S.-based example, see the Cybersecurity Capability Maturity Model (C2M2) available at https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[113] Available at https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

[114] One such example of the integrating ISO 27001 standards can be found in the Republic of Moldova: https://a.cec.md/storage/old_site_files/files/files/20%20ani%20CEC/Cartea_Cec_20_ani_eng_compressed.pdf

The following sections will use the electoral cycle, an established heuristic, to discuss threats, vulnerabilities, and mitigation across the electoral process. It is helpful to view the mitigations discussed below through the lens of the three previously-introduced, basic control types: management, operational and technical. These control types can be integrated into mature risk management mechanisms tailored to the electoral context. Given the dynamic nature of cybersecurity, and the multiplicity of contexts EMBs around the world face, this discussion is not, and cannot be, comprehensive. Instead, this discussion will first highlight how the idea of risk management can be introduced to clarify the challenge of cybersecurity for EMBs and will then identify areas where further guidance is needed. Before introducing the election cycle, the next section presents a short discussion of cyber adversaries.

A. Threat Actors

Any discussion of cybersecurity will be incomplete without a discussion of threat actors; defining risk means understanding, as fully as possible, the adversary. This discussion will define categories of actors and speak briefly about the types of tactics, techniques, and procedures (hereafter refered to as tactics) employed by such adversaries. TTPs, as a concept, are used within the broader security community (both physical and cyber) to define the universe of techniques and associated actions malicious actors employ to achieve their intentions. TTPs are important to consider as, often, certain mixes of techniques, tactics, and procedures can distinguish certain threat actors from others. In addition, risk management frameworks use comprehensive understanding of TTPs to engineer controls to provide holistic defense mechanisms. The discussion of cybersecurity TTPs can easily extend into granular technical dimensions; as such, this report will only provide an introduction of how various threat actors employ and favor specific methods, tools, and actions.

DRAFT

Disinformation as a tactic to undermine public confidence has emerged as a key component in this space, especially since 2016. Populist politicians in developing countries have long sought to blame election technology vulnerabilities for their electoral defeats, but this trend has now also taken hold in major consolidated democracies — both in the pre- and the post-electoral context. The fallout of such demagoguery has led to multi-million dollar tort suits by the election technology industry.[115] Worse, it has eroded public confidence in elections among large segments of the electorate.[116] While it remains true that election technology cannot be completely protected against cyber threats, the lines between hypothetical residual vulnerabilities and successful cyber attacks have blurred in the public consciousness.

Within each broad category there are entities that are seeking to disrupt and undermine public confidence in elections, or to prevent a periodically scheduled election from taking place, either to extend their own mandate, or to thwart the overall democratic process. Over the last decade, the array of threat actors has widened considerably.

1. Foreign State Actors and Advanced Persistent Threats~~APTs~~

[115] https://www.businessinsider.com/everyone-dominion-smartmatic-suing-defamation-election-conspiracy-theories-2021-2?op=1

[116] https://morningconsult.com/form/tracking-voter-trust-in-elections/

Malicious actors associated with or directly tied to foreign governments constitute a grave threat within the election security space. These groups are well-resourced and utilize sophisticated techniques. The level of sophistication is described by the term "Advanced Persistent Threat" or APT, and there are different industry and government designations for important threat actors.

Among actors that can sustain and execute cyber operations at the APT level, two - designated APT 28 and APT 29 respectively - are worth discussing further. APT 28 ,also known within the industry as "Fancy Bear," is part of Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center.[117] APT 29, also known within the industry as "Cozy Bear," is attached to the Russian Foreign Intelligence Service (SVR).[118] Both groups have been responsible for some of the highest visibility and effective cyber operations against elections entities over the past several years.[119] Identifying operations carried out by APT 28 and APT 29 relies, in part, on assessing the TTPs utilized. These operations are characterized by sophisticated methods that make use of "zero-day exploits" to gain and sustain access to information systems. Zero-day exploits are so named since they take advantage of vulnerabilities that the larger cybersecurity industry is not aware of and thereby cannot be easily defended against. Both groups have access to a large supply of zero-days that highlight their relationship to government resources, such exploits would require sustained research and experimentation to identify.[120]

In addition, these well-resourced groups are able to use their state-level intelligence relationships to engineer sophisticated "spear-phishing" operations targeting high value individuals. Spear-phishing is a targeted variant of the tactic of "phishing" where an adversary tries to harvest credentials and passwords from unsuspecting users by tricking them. Usually this involves sending an email with a malicious attachment or crafting webpages designed to capture user credentials and relies on unsuspecting victims believing the web page/email is legitimate. APT level threats use sophisticated intelligence and reconnaissance techniques to craft content presented to the target in a way that makes it hard for victims, even persons that have had training, to distinguish the malicious content from legitimate communications. APT 28 and 29 have operated since the mid-2000s and their efforts have often been geopolitically targeted at undermining the credibility of democratic and, later, electoral systems, therefore posing a considerable threat to public trust. China, Iran, and North Korea all have sophisticated offensive cyber operations that leverage APT level tools, tactics, techniques, and procedures.[121]

DRAFT

2. Government Actors

Government actors often work against certain electoral stakeholders within their own state, particularly in countries that are electoral autocracies or have characteristics of this typology.[122]

---

[117] https://attack.mitre.org/groups/G0007/ and https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[118] https://attack.mitre.org/groups/G0016/

[119] https://www.wired.co.uk/article/how-russian-hackers-work

[120] https://www.wired.co.uk/article/how-russian-hackers-work

[121] https://www.mandiant.com/resources/apt-groups

Their efforts are often targeted at undermining the credibility of certain political or civil society actors, especially where there is a possibility of them making inroads through electoral processes. Instances have been noted in places like the Russian Federation, Belarus, Africa, South-East Asia, and all across Latin America.[123] These actors can work independently, but also sometime coordinate with clandestine services, criminal or independent groups to achieve their aims.

3. Criminal Groups

Criminal groups are often involved in cyber crime for financial gain (for instance, ransomware attacks against state institutions). There is little official record of EMBs paying a ransom to recover its data, and it seems that in most cases, election administrations were collateral damage from larger attacks on government infrastructure.[124] Sometimes, however, it is suspected that criminal groups will work in concert with governments or foreign threat actors for either financial renumeration, political motivation, or due to pressure placed upon them. They have also been used by government actors to evade attribution. The willingness of cyber-criminal groups to "sell" their expertise and resources has given rise to the term Cybercrime as a Service (CaaS). Criminal groups will, for example, "rent" their command and control of infected computers to direct requests that, through request overload, cause servers to crash. This type of attack is called a distributed denial of service or (DDoS). It should be noted that modern sophisticated criminal groups can utilize TTPs that sometimes approach or mirror the sophistication of state sponsored actors. This means that APT level sophistication can, potentially, be purchased and utilized by both state and non-state actors that do not themselves possess the resources for such attacks.[125]

DRAFT

4. Insider threats

Individual or collective threat actors might also operate from within EMBs. Understanding the motivations of insiders that decide to act against the interests of their employer is difficult. However, a key component of any comprehensive cybersecurity program is to assess the threat of – and put into place controls for – insider threat mitigation. Insider threat within the context of EMB operations is still poorly understood and thereby even more difficult to detect and/or address. There are, however, managerial, operational, and technical controls that are designed to help mitigate such threats. For example, sensitive IT processes should utilize "two-person" control whereby two people have to sign off and be involved to successfully complete the task. Another administrative (management) control would be the execution of background checks for EMB employees to help screen out candidates that are more likely to pose insider threat. In terms of technical controls, automated alerting of suspicious activity such as copious printing

---

[122] See https://www.v-dem.net/files/25/DR%202021.pdf

[123] https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[124] State of Georgia, USA, 2020 https://edition.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html and North Macedonia, 2019 https://www.osce.org/files/f/documents/1/7/428369_1.pdf

[125] Bitdefender, More Evidence of APT Hackers-for-Hire Used for Industrial Espionage, available at https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

outside normal business hours can be utilized to help identify possible exfiltration of data by insiders. These types of controls may not be achievable given the resources available to certain EMBs.

IV. Election Stakeholders

Subsequent sections of this report will focus on the EMB perspective while highlighting technology usage across the electoral cycle. Before doing so, the concept of multi-stakeholder coordination will be discussed and two important electoral stakeholder groups that have been the focus of threat actors will be highlighted: civil society organizations (CSOs) and political parties.

A. Multi-stakeholder coordination

There are various models of interagency collaboration during elections, including on transportation, security and public health, that are essential to the credible election administration. Although there are some good examples of multi-stakeholder coordination in the realm of election security – for example, the 2020 U.S. elections in which CISA played a critical supporting role to local and state-level election administrators and the coordination in the 2019 Ukrainian elections between the Ukrainian security services and the Central Election Commission (CEC) – the field is under-studied and would benefit from more research. Ensuring effective cybersecurity in elections in particular may necessarily transcend the traditional mandates and capacities of institutions – particularly EMBs. Effective cybersecurity may require resources that an EMB is unlikely to be able to gather on its own, as well as a comprehensive threat awareness and detection/deterrence capability that requires information and data exchange and response from multiple agencies.

DRAFT

There are multiple models of multi-stakeholder collaboration (formal or informal). Some are purely inter-agency, involving different government departments and independent institutions such as the EMB. Others include state and non-state agencies (including private sector vendors, social media providers, media and academia). Some coordination efforts are organized into thematic task forces (for example, a disinformation task force, or an online voting task force, while others focus on specific parts of the electoral process (for example, collaboration on training of poll workers ahead of elections, or collaboration via a "war room" to track threats on Election Day itself). The specific political and institutional context – as well as the specific resource needs and vulnerabilities – will dictate the best mode of collaboration between multiple agencies and stakeholders on issues surrounding cybersecurity.[126]

A critical consideration around multi-stakeholder coordination is the fact that the independence and the perception of independence of the EMB must be safeguarded. Hence, any interagency collaboration should be publicly explained in a transparent and clearly defined manner. Each party that is engaged during cybersecurity activities must agree on the terms and context of that engagement. This is usually done through defined rules of engagement. Rules of

[126] See, for example International IDEA's Models of Interagency Collaboration available at: https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

engagement provide a defined framework for how different actors and institutions will respond to identified cyber-threats. The intervention (or non-intervention) of government agencies during an ongoing cyber-attack can be, in some countries and in some contexts, politically charged. Accordingly, clear rules should be determined in advance and communicated to all election stakeholders. These rules should be sufficiently detailed so there is no ambiguity with regards to roles and responsibilities, while giving sufficient leeway for actors to efficiently respond to an incident in a coordinated way. A balance must also be struck between transparency of any cybersecurity response, and the security of the protective measures themselves, to limit opportunities for bad actors to capitalize on freely available information about election cybersecurity platforms and processes.

Successful interagency collaboration and coordinated incident response will depend on whether there is a common understanding of roles, responsibilities and communication channels. Technical simulations or strategic tabletop exercises can help organizations by rehearsing these roles and testing these channels, while also allowing those organizations to build and refine incident response mechanisms and procedures outside of (and well before) in the high stress environment of an electoral event.

B. Civil Society Organizations

Civil society plays a vital role in supporting government accountability and civil society organizations (CSOs) that are focused on elections can help inform the public about a range of electoral issues – including the security of voting data and processes. Moreover, CSOs that understand election technology and its associated benefits and risks can provide an external perspective on key technology or cybersecurity decisions made by the government, legislature, or election officials and offer informed, independent advice, ideally helping to strengthen EMBs and elections more generally. This advice can help officials consider the end users of election technology and information needs that may need to be built into poll worker training or voter education.

DRAFT

In many countries, national and local CSOs play a key role in ~~technical~~ oversight of the electoral process, and election-day observation. Citizen (domestic) election monitoring efforts can help encourage adherence to election procedures, improving public confidence in the integrity of the election (when warranted). However, given the sensitivity of election monitoring in some countries, and the potential political impact of such reporting, there are some cyber security vulnerabilities for CSO observers. This can include the insecurity of databases containing observer information (such as names, locations, email addresses, phone numbers). Databases containing observers' personally identifiable information (PII)[127] are vulnerable to breach of confidentiality. The integrity of observation data and draft observation reports could also be undermined if no safeguards are in place. For example, when default accounts and credentials (often put in place by software/hardware providers for initial configuration) that have not been further secured remain in place and are accessed by users, data can be compromised and used by adversaries.[128] Finally, the transmission of observer reports and communications via insecure

[127] McCallister, E. (2010). Guide to protecting the confidentiality of personally identifiable information (Vol. 800, No. 122). Diane Publishing.

methods of communication can prove vulnerable to interception, for example if such reports are transmitted via common, unencrypted email.

These vulnerabilities, if exploited, can reduce public trust in the integrity of a given CSO, and in the broader election process. It can also leave CSO staff and observers vulnerable, particularly in repressive or closing political environments where CSOs may be under broader attack or scrutiny. As such, it is important for CSOs to maintain strong control of their internal communication and to protect the secure nature of their privileged relationships with key government partners. Hostile actors can gain access to such communication, often through phishing or spear-phishing attacks on CSO staff,[129] brute force attacks (where hackers attempt to guess a password to gain entry to a CSO's internal communication systems),[130] or communication interception through the exploitation of insecure WIFI networks or other unsecure channels.

To mitigate these risks, CSOs should implement organization-wide cybersecurity measures, starting with robust cyber hygiene training that can help reduce the likelihood and impact of common attacks. CSOs should also prioritize using full disk encryption on hardware and physical security tokens, especially if working in politically hostile environments. Finally, CSOs should seek to reduce or eliminate information and data exchange via insecure means of communication, such as SMS or public WIFI networks, and instead use~~mandate~~ end-to-end encrypted messaging platforms.[131]

C. Political Parties

DRAFT

Regular internal communication and electronic information exchange are integral parts of the day-to-day operations of a political party. These communications can span a wide range of topics, some politically sensitive – such as draft policy positions, opposition research and campaign strategies – and some involving personal information – such as personal vetting documents and correspondence with donors. The systems used for these communications can vary widely and include email accounts, cell phones, landlines, SMS text messages, third-party messaging applications, web-based platforms, computers, databases, smartphones and mass messaging applications.

Additionally, in many democracies political parties are comprised of tens of thousands of members, and sometimes affiliate groups associated with the party. Political parties need to store information for all the members associated with their party, including PII and donor contributions and expenditures. They typically store this information in a database or customer relationship management (CRM) solution, both of which could be susceptible to cyber attacks. Accordingly, parties should secure these information storage solutions using encryption and industry standard protections.

---

128 https://us-cert.cisa.gov/ncas/alerts/TA13-175A

129 https://www.cisa.gov/sites/default/files/publications/NCSAM_Phishing_2020.pdf

130 https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

131 Ermoshina, K., Musiani, F., & Halpin, H. (2016, September). End-to-end encrypted messaging protocols: An overview. In International Conference on Internet Science (pp. 244-254). Springer, Cham.

Given the sensitivity of party communication and information, and the potential for data misuse, political parties can be particularly vulnerable targets for cyber attack. In 2016, operatives hacked the server of the Democratic National Committee (DNC) in the United States. Twelve Russian military officers were charged with breaking into the Democratic Party's computers, stealing compromising information and selectively releasing it to undermine specific candidates.[132] Members of the German *Bundestag* were targeted with phishing attacks on their email accounts in 2015, and again in 2021 in the run-up to parliamentary election, in what was suspected collusion between right-wing domestic groups and the Russian GRU.[133] The French *En Marche* political party's handling of a 2017 breach in their communications provides an example of a sophisticated and effective response: the party's IT team identified the breach in its early stage and applied a strategy of *cyber-blurring*, injecting fake information and creating fake accounts among legitimate, though compromised, accounts. This action slowed the efforts of the adversaries without alerting them to the fact that they had been detected, ultimately reducing the value of the data that was exfiltrated.

Political parties must also manage a number of additional risks. These include the risk that insufficiently trained staff and volunteers are not able to recognize and avoid cybersecurity threats like those posed by phishing and social engineering attacks., There is also the risk that communication via insecure computers and smartphones will be intercepted or compromised. Insiders with malicious intent can pose a threat as well.[134] To combat these threats and mitigate risks, political parties should regularly conduct cyber hygiene training, ensure that party email accounts have spam and phishing protection, enable full disk encryption on all hardware (to include the use of physical security tokens), use end-to-end encrypted communication platforms, and configure data loss prevention software for all sensitive documents and data. Beyond stop-gap measures to improve their security postures, political parties should consider hiring dedicated cybersecurity staff at least during campaigning periods and should strive to implement holistic cybersecurity risk management programs. Facing sophisticated and persistent adversaries will require political parties to be agile and to understand both risk mitigation and incident response – knowledge they are unlikely to acquire without the aid of external experts.

DRAFT

Finally, both political parties and CSOs (as well as other stakeholders) should take note of the recent Pegasus leak, which revealed widespread use of cyber-surveillance tools by governments.[135] The information that has emerged from the leak shows that governments can

---

[132] https://www.cbsnews.com/news/russian-hackers-2016-election-democratic-congressional-campaign-committee-60-minutes-2020-08-23/

[133] https://www.zeit.de/politik/deutschland/2021-03/cyberangriff-russland-hacker-bundestag-ghostwriter-geheimdienst-gru-cyberwar

[134] Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. J. Wirel. Mob. Networks Ubiquitous Computer. Dependable Appl., 2(1), 4-27.

[135] Pegasus is spyware sold by the Israeli company NSO Group which allows surveillance of mobile communications. It is marketed as a tool for monitoring criminal activity, but has been used by governments to monitor and target CSOs, journalists, activists and members of political opposition parties deemed controversial or threatening to ruling governments. The Pegasus Project (led by Amnesty International, Forbidden Stories and the Organized Crime and

procure and use sophisticated cyber methods to monitor the activities of their political opposition, as well as journalists and civil society members that operate in their countries. High profile political targets should call upon specialized agencies or vendors to secure their devices; otherwise, as a protective measure, they should assume their devices are compromised and engage in communications accordingly.

The next sections in this paper highlight the use of technology throughout the electoral cycle from the perspective of election management bodies. The types of risks and vulnerabilities that are present can also be applied to CSOs and political parties. As such, the types of security controls and mitigations discussed can also be utilized by these entities as they endeavor to mature their own cybersecurity postures.

V. The Electoral Cycle

As characterized earlier, the election process is complex and multifaceted, while also varying across democratic systems and contexts. ~~It is reductive to think of EeE~~lections are not~~as~~ simply procedural in nature. Rather, an understanding of electoral dynamics should account for interactions through various stages between an EMB, political parties, civil society, state apparatus and media, among other imp heuristic that helps drive this more hc cycle helps guide election managers to post-election period, each having certai into one another. The cyclic depiction s execution of the current election, an measured in years – as the process m Figure 1 may rely on information techn tasks across the electoral cycle, an EMB over some subset of that IT infrastruc execution of an election involves inforn an obvious threat vector is highlighted: t



This fundamental need for coordination and information flow among disparate stakeholders can be characterized as happening across *seams*. Seams are defined as the gap across which information must traverse and coordination must occur between two or more distinguishable functional units (for example an EMB, central government, and municipalities). Preventing the successful coordination and flow of information across these seams by targeting the confidentiality, integrity or availability of information is a likely tactic that an adversary may choose to utilize. Since much of that information and coordination may happen via electronic

Corruption Reporting Project) aims to expose how Pegasus is being exploited. See https://www.occrp.org/en/the-pegasus-project/.

information technology, cybersecurity must be a central consideration for EMBs.[136] While the implication of disrupting the election process via seams is understudied, the concept of multi-stakeholder collaboration has been an area of focus.

The next sections will highlight the technologies and processes involved with various important tasks within the election cycle, with an emphasis on cybersecurity risks, threats, -and mitigation strategies. The discussed controls should be viewed as good practices that can be replicated and utilized across an EMB's information technology infrastructure and developed further as EMBs mature their cybersecurity risk management practices.

A. Pre-election Period

1. Legal and Regulatory Context

Many EMBs introduce election technology with little or insufficient adjustment of the legal or regulatory framework for elections or are compelled to introduce technology due to imperatives added to the law. This can cause significant problems in practice; for example, due to tight procurement timelines to meet legally mandated election dates, which result in little time for testing and training (or leads to criticism of the EMB for undertaking emergency procurement or sole sourcing). In addition, some regional principles prohibit amending fundamental elements of the legal framework in election years, as in the Council of Europe and Economic Community of West African States (ECOWAS) regions. This results in countries attempting to implement new operational paradigms within existing, outdated legal frameworks. This is problematic, as legal frameworks are crucial for defining the powers of -– and imposing duties of care on – EMBs and EDR tribunals around the deployment and use of election technology.

DRAFT

At a minimum, the following issues should be considered in the legal and regulatory frameworks for election cybersecurity:

1) Responsibilities and liabilities of the vendor vis-à-vis the EMB in terms of cybersecurity;
2) The actor responsible for auditing, testing and certifying election technology before its deployment; transparency of these processes; and how cybersecurity considerations are weighed and considered;
3) The institutions with access privileges and duty of care in the use of election technology;
4) Protections for the data privacy of election stakeholders; the legal value of electronic election data vis-à-vis data recorded on paper (especially results data); and the impact a cybersecurity breach may have on the validity of results;
5) Requirements for EMBs and EDR tribunals to ascertain ex-post that election technology was not successfully penetrated by cyber attacks;
6) What actions or processes (e.g., an audit, full recount, annulment and rerun) a detected cyber attack would trigger;[137] which institution would oversee these processes (the EMB

[136] The concept of seams is discussed in detail within and adapted from Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: the cybersecurity coordination problem. Journal of Cybersecurity, 4(1)

[137] See for example: https://www.nytimes.com/2017/09/01/world/africa/kenya-election-kenyatta-odinga.html

or the EDR court, or the national cybersecurity agency); whether private sector, third parties are allowed to conduct testing and audits (as is the case in Iraq);[138] whether election technology equipment would be considered to be compromised once it is accessed by a third party (as was the case in Arizona in 2021);[139] and

7) The cyber security standards that must be met when procuring election technology, and ownership and access permissions for the source code; the procedures for replacing a compromised EVM.

These considerations help clarify the challenge of adapting existing cybersecurity risk management frameworks and controls to the EMB context. While managerial and operational controls used in business and government agency operations are relevant – including privacy, access privilege, and duty of care – they must be clarified for the electoral context. The post incident response process also needs to be considered, as the electoral context may demand a more transparent investigation than a private company or government agency might otherwise undertake once a cybersecurity incident has been detected and verified. Elections are fundamentally public exercises, and as such, while EMBs can strive to use risk management-based frameworks for cybersecurity, there is much work to do to sufficiently tailor and define specific mechanisms and controls for the electoral context.

Good practice would allow EMBs and legislatures sufficient time to adapt the legal and regulatory framework prior to~~in the wake o~~f technology procurement, so that it sufficiently takes into account powers and duties to ensure cybersecurity, and sets out a framework for contingency measures in the event that a successful cyber attack occurs. The Council of Europe *ad hoc* committee on electronic voting recommends that, "There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, maintaining, observing and auditing e-voting systems. (…) It is recommended that the relevant legislation provides for the supervisory role of the electoral management body over e-voting. The role and the responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level."[140]

DRAFT

The absence of governing legal frameworks and legislation opens EMBs to risks that go beyond cybersecurity as well. For example, in March 2016, the Philippines Commission on Elections (COMELEC) was hacked by a group called Anonymous Philippines. The hackers took over COMELEC's website – which was temporarily shut down in the aftermath – and released extensive voter information, including fingerprints. Following the attack, the National Privacy Commission recommended criminal charges against COMELEC Chairperson Andres Bautista for negligence. In its decision of December 28, 2016, the Commission stated that "the willful and intentional disregard of his duties as head of agency, which he should know or ought to know, is tantamount to gross negligence. The lack of a clear data governance policy, particularly in

[138] https://reliefweb.int/report/iraq/iraq-s-electoral-preparations-and-processes-report-no-11-9-september-2021, see also for perspective from a different country context: https://www.telesurenglish.net/news/Ecuadors-Comptroller-to-Audit-Electoral-Computer-System-20210221-0003.html

[139] https://www.nbcnews.com/politics/elections/maricopa-county-will-need-new-voting-machines-after-gop-s-n1268090

[140] Standard 29: https://rm.coe.int/168071bc84

collecting and further processing of personal data, unnecessarily exposed personal and sensitive information of millions of Filipinos to unlawful access."[141]

While the Commission did not find Bautista guilty of helping with the attack, it did establish a precedent of holding EMBs and their leadership accountable for information security failures and data breaches in elections. The Commission ordered COMELEC to implement new security measures, conduct a privacy assessment, appoint a Data Protection Officer, and establish a Privacy Management Program and a Breach Management Program. Less than a month later, a computer was stolen from the Office of the Election Officer (OEO) in Lanao Del Sur, which the National Privacy Commission noted was "COMELEC's second large-scale data breach in a span of less than a year."[142] The computer contained biometric records of registered voters. Chairperson Bautista was impeached in October 2017 and resigned that month. Bautista was accused of mishandling the data hack, receiving payment from the company whose voting machines were used in the 2016 elections, and failing to disclose his assets. The Philippines case is a compelling example of potential institutional and personal liability for EMBs and election officials with respect to cybersecurity in elections, and of the role that privacy commissions may play with respect to oversight of personal data in elections.

The electoral legal framework may present a challenge for the introduction of new technology in the electoral process. The relevant legal provisions may reside in three locations: "the constitution, if there is one, the laws relating to elections (or articles in general laws related to elections, such as for example, the criminal code), and the secondary legislation (such as regulations, rules and procedures often passed by EMBs)."[143] In some cases, legislation governing these technologies may be found in areas outside of elections, such as regulations on data protection.[144] Before working within the existing framework of laws and regulations, it is necessary to address "not only the tools needed, but also the systems and processes that must be reengineered in order to shape an effective solution."[145] As noted by the Council of Europe, any changes to the legal and regulatory system should be accompanied by clear, public explanations of why those changes are necessary, which "will reinforce voters' and other stakeholders' trust and confidence."[146]

DRAFT

In addition, the country's specific election system must also be considered before implementing new election technology. For example, before using new technology for voter registration, it is important to know who registers voters (the EMB, another government agency, or another organization), who collects data on voters, how that information is shared with the EMB (if the EMB does not collect the data), and who owns the data.[147] New technology typically requires

---

[141] https://www.privacy.gov.ph/2017/01/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/

[142] https://www.privacy.gov.ph/2017/02/npc-starts-probe-comelecs-2nd-large-scale-data-breach-issues-compliance-order/

[143] Goldsmith and Ruthrauff, Implementing and Overseeing Electronic Voting and Counting Technologies, 106.

[144] OSCE, Guidelines for Reviewing the Legal Framework for Elections, 2nd ed., 2013, 65-69.

[145] Yard, ed., Direct Democracy: Progress and Pitfalls of Election Technology, 21.

[146] Council of Europe, Guidelines on Transparency of E-enabled Elections, 2011, 5, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf6.

additional human capital considerations, such as stronger information technology (IT) skills and experience. Many election staff often lack the skills to manage new technology without training.[148] In Kosovo in 2010, local staff were found to need two electoral cycles' worth of training before they would have the IT skills and experience necessary to run the relevant technology on their own.[149] This highlights the security risks around poorly equipped technology users who may be easy targets for malware on individual terminals that are connected to wider systems and networks.

An appropriate timeframe for procurement, implementation, testing, and training is also a decisive factor in determining whether to use a new technology. Timelines for ensuring a smooth transition to new technology will vary by country and electoral cycle. EMBs should have a clear plan, from the initial determination of the technology's merits as applied to the electoral process through final implementation. Introducing new technology too quickly can jeopardize public trust and can lead to technical challenges, further eroding trust in the process.[150] A fundamental part of this process that is often inadequately factored into planning is the testing process, which should be part of standard operating procedures. Another key factor to consider is whether there will be a process of systems integration, usually between hardware and software, or the wholescale introduction of new hardware and software into an electoral process. Both can produce vulnerabilities, but systems integration can give rise to unique challenges, particularly where a new solution is essentially bolted onto an existing system or platform.

DRAFT

The level of public trust and confidence in the electoral process and the EMB specifically must also be taken into account when deciding whether to implement new election technology.[151] If public trust in the electoral process is already low, introduction of a new system may cause public unrest.[152] Rather, technology should be introduced at a stage when all electoral stakeholders enjoy significant trust in the process, rather than attempting to use technology to mask the problems. To build trust, the Council of Europe recommends public debates or consultations that include all voters. These public outreach activities should lead not only to greater trust in the technology itself but to greater trust in the implementers of the new technology. International IDEA's recommendations include releasing the results of pre-implementation testing, auditing the new technology regularly, and developing and publicizing clear policies "that cover all aspects of technology use."[153] Specific tools that provide independent ways to test the system, such as audits of technology systems, are also a good

---

[147] Michael Yard, ed., Civil and Voter Registries: Lessons Learned from Global Experience, 2011, 8; European Commission, Methodological Guide on Electoral Assistance, 2006, 59-60.

[148] Yard, ed., Civil and Voter Registries: Lessons Learned from Global Experience, 157.

[149] Ibid., 42.

[150] European Commission and UNDP, Procurement Aspects of Introducing ICT Solution in Electoral Processes, 2010, 55.

[151] European Commission, Methodological Guide on Electoral Assistance, 57.

[152] Council of Europe, "Guidelines on the implementation of the provisions of Recommendation CM/Rec (2017) 5 on standards for e-voting," CM-Rec(2017)50, June 14, 2017.

[153] Helena Catt, et al., Electoral Management Design, revised ed., International IDEA, (Stockholm, Sweden: 2014) 266-267.

means to gain public trust and secure against fraud.[154] Public communication around contingency planning is also fundamental so that changes in procedure – for example, switching to paper ballots in case of a power outage or security breach – are not perceived as suspicious in and of themselves.

Comprehensive cybersecurity makes use of several controls, as outlined above. Those measures must also be considered alongside additional mechanisms that may be built into the law to help maintain confidence in the results of elections that leverage technology. One example is tabulation audits, which review a set of ballots, interpret voter intent and check that determination against the results produced by the original tabulation process.[155] Risk-limiting audits (RLA), a type of tabulation audit that relies on statistical evidence to confirm the outcome of an election, are increasingly used in the U.S. context to confirm the machine count.[156] As with other audits, changes may be required in the law and procedures to accommodate the RLA. Specifically, IFES has indicated that the laws should:

- Clearly define the purpose and parameters of the risk-limiting audit;
- Specify how contests are selected to be audited;
- Select an appropriate risk limit ("the predetermined maximum probability that the audit will not uncover an incorrect outcome") or delegate authority for its determination;
- Ensure the timeframe for the RLA is compatible with legal deadlines for election counts and results certification, and that the audit is appropriately harmonized with election dispute resolution processes;
- Provide for public accessibility and verifiability of the entire RLA process; and
- Require security and integrity measures, including appropriate ballot accounting procedures.[157]

DRAFT

5. General election administration and planning

Overview and main uses of technology: Election administration is a continuous process throughout the electoral cycle. Identification and mitigation of risks and vulnerabilities must be considered from the start of the process, which is often two years or more before Election Day, and continues toward the next cycle. This stage of the electoral cycle includes procuring information and communication technology (ICT) systems, websites, social media and communication platforms; and managing physical locations, personnel, training and budgeting. Proper security planning and field-testing with the necessary cybersecurity, law enforcement, military, and private security stakeholders is also important throughout all phases of the electoral cycle. State election laws in the U.S., for example, require election equipment testing and certification by government-accredited agencies, but most countries that acquire election technology lack such a framework.[158] Many countries also do not allow independent

[154] European Commission, Methodological Guide on Electoral Assistance, 63.

[155] https://www.ifes.org/sites/default/files/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf

[156] https://www.ifes.org/sites/default/files/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf

[157] https://www.ifes.org/sites/default/files/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf

[158] https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

observation of election technology testing, which detracts from stakeholder confidence in that technology's protection against cyber attack.[159]

Procurement processes have often been cut short, because of time constraints or EMB relations with favored vendors, which has curtailed effective bid evaluation of cybersecurity criteria. Cybersecurity is also often given insufficient attention when drafting technical specifications for tenders, and cybersecurity experts are seldom called upon to serve on tender selection committees. Cybersecurity field-testing or penetration-testing is rarely performed prior to bid selection and contracting. In Pakistan, a Senate Committee recently rejected acquisition of EVMs on grounds of governance issues, as well as cybersecurity.[160]

Risk discussion: Personnel who use, interact with, or access electoral ICT systems may lack proper cybersecurity awareness to evaluate leading threat vectors such as social engineering and phishing incidents. Systems and infrastructure may not be designed with cybersecurity in mind, leading to vulnerabilities that allow for successful intrusion, and the ability to pivot to other network segments or other connected infrastructure once the system has been breached. Election data and non-election information might be at risk of data-loss that could delay multiple stages of election preparation. When cyber attacks occur, personnel may not understand their roles, leading to mismanagement of a cyber incident. Proper interagency communication and collaboration channels may not be in place, leading to ineffective responses. Electronic security plans could be exfiltrated and used by malign actors to bypass existing security control mechanisms.

DRAFT

Mitigation strategies: EMBs should consider cybersecurity an organizational requirement, rather than an ICT problem. EMBs are advised to progressively integrate cybersecurity good practices, with regular assessments of their posture and a risk-based approach to adopting new technologies, including in their strategic and operational planning and budgeting. The various institutions and agencies associated with these general election administration and planning processes should implement risk management and security controls according to the ISO, NIST, ENISA or other frameworks. It is imperative for EMBs to develop cybersecurity education and awareness training, and to test user readiness with simulations.[161] They should also engage with other agencies responsible for the cybersecurity of other aspects of these processes that fall outside of the EMB's purview, creating efficient communication and response channels and plans.[162]

EMBs should use the concept of *least privilege* as part of their operational and technical controls. This helps ensure that only persons who are authorized, and who need access, can access sensitive information. Further controls can be used to implement comprehensive data loss prevention programs; such programs combine managerial, operational and technical

[159] https://www.golosinfo.org/articles/144545

[160] https://tribune.com.pk/story/2319515/senate-body-rejects-use-of-evms-in-next-elections

[161] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237-248.

[162] Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. Computer Fraud & Security, 2021(1), 14-19.

controls to maintain control of data as it traverses organizational boundaries, and to prevent proprietary data from leaving designated infrastructure.[163] In addition, EMBs should create clear policies that define acceptable use of technologies within the organization (e.g., requiring all personnel to use an official, institutional email account – the infrastructure of which is under EMB control – for all communications). Finally, EMBs should embrace cybersecurity as a central procurement criterion and adjust their procurement timelines and procedures accordingly, while also formalizing the cybersecurity requirements that flow down to contractors.

6. Boundary delimitation

Overview and main uses of technology: The boundary delimitation process refers to drawing electoral district boundaries (or constituencies). It also involves determining electoral precincts and polling locations and assigning voters accordingly. Boundary delimitation typically takes place in the pre-electoral and post-electoral phases.[164] Technology has been increasingly integrated into these processes to map locations and to distribute voters equitably to maintain good practice standards of vote weight, including impartiality, equality, representativeness, non-discrimination and transparency. [165] As a result, technology has mostly replaced cumbersome manual processes.

Risk discussion: The integrity of boundaries and voter distribution may be vulnerable if data (for instance, geographical information systems databases) are externally facing (connected to the internet) for ease of access. Interconnectivity with other state institutions, such as census institutions or ministries responsible for population, also represent vectors of possible compromise. Additionally, the technologies and components used for activities such as drawing boundaries or for assigning voters to specific polling locations may not incorporate the ability to log and audit the actions taken by various users. Without such features, EMBs or the responsible boundary delimitation authority may not be able to locate the source of mistakes or problems as they arise.

DRAFT

Mitigation strategies: When systems are interconnected to outside entities, EMBs should create formal agreements such as "service level agreements" (SLAs) and memoranda of understanding (MoU) to define the relationship and responsibilities of each party involved. In terms of security controls, these agreements should specify cybersecurity requirements and post-incident standard operating procedures to help distinguish responsibilities in case of breach. For example, if an EMB's systems are infiltrated due to connection with a census bureau, does the EMB have the right to inspect the bureau's systems during the investigation? In addition, data exchange should make use of integrity checks to ensure the data received is unaltered from the data transmitted. Technical controls, such as utilizing automated logging and audit solutions where possible, should be implemented along with data encryption both at rest and during transmission.

---

[163] Liu, S., & Kuhn, R. (2010). Data loss prevention. IT professional, 12(2), 10-13.

[164] Handley, L. (2007). Boundary Delimitation. Challenging the Norms and Standards of Election Administration, 59-74.

[165] Handley, L. (2007). Boundary Delimitation. Challenging the Norms and Standards of Election Administration, 59-74.

7. Voter registration

Overview and main uses of technology: Voter registration (VR) processes are comprised of databases related to storing and managing voter registry data, as well as digital components and processes related to registering voters. At their core, all voter registration systems are structured on databases that contain voters' PII. The degree of automation and the range of services varies depending on a country's legal framework, and the election administration's eagerness to deploy new technologies.

The need to eliminate duplicate voter registrations has made it essential for EMBs to digitize the voter registration process (or to enhance it with biometrics), and today nearly all voter registries in the world are hosted within electronic databases. Most countries operate nationwide voter databases, making them critical infrastructure that could be targeted by cyber attacks.[166]

Several attacks against the confidentiality, integrity, inclusivity and availability of voter lists before and during elections have demonstrated the potential for disruption and damage. Some of the largest data breaches recorded worldwide have been voter list databases, severely impacting the credibility of EMBs.[167] In the U.S., many states register voters by party, making U.S. voter databases especially attractive targets, as a successful compromise can be used to exacerbate partisan cleavages and direct information campaigns based on party affiliation. In addition to allowing online verification of voter registration, many U.S. States have begun to allow online voter registration, and most states have also begun allowing absentee ballot applications online.

DRAFT

Risk discussion: Identifiable risks include breaches or misconfiguration of online cloud storage housing voter registration databases, leading to the exfiltration of sensitive data. Because offline voter registration collection processes are still fairly common in most parts of the world, laptops or portable media are often used to locally store and transport voter information, making this equipment an attractive commodity if physically stolen. EMBs should consider the cybersecurity risks associated with the integrity of voter registration (both traditional and biometric), including remote access to databases published online, unprotected data transmission from field-deployed voter registration equipment to a central database, and integrity issues related to equipment compromise in the supply chain prior to delivery. When voter verification equipment, such as electronic poll books, are connected to the internet, compromise could lead to voter suppression or a voting disruption.[168] Because voter registration systems have public-facing components, such as information published online for public viewing, there is a risk that denial of services attacks can undermine voters and political

[166] The U.S. lacks a nationwide database. While some states have state-wide databases, others rely on each county to maintain their own database. This makes VR a less attractive target in the U.S., but also multiplies the cybersecurity effort required to safeguard the myriad U.S. voter databases from attack.

[167] Comelec: No biometrics in leaked data, https://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.htmland Voter database made accessible online, 87 million voters from Amazon Web Services (Mexico) https://www.scientificamerican.com/article/mexico-s-entire-voter-database-made-accessible-on-the-internet/

[168] https://www.govtech.com/security/digital-poll-book-failures-slowed-voting-in-several-states.html

party trust in the voter register, or in the election authority's credibility as a professional custodian of democratic elections.

Mitigation strategies: To mitigate these risks, EMBs should: disable remote access to these systems where possible (this is difficult when voters proactively exercise functions online that must be authenticated and validated by the voter register database, such as absentee ballot requests or online voter registration, as is becoming more common in the U.S.);[169] employ designs that segment systems from the rest of the network using current generation firewalls; use a third-party risk management process; and employ a patch management strategy that ensures timely closure of known vulnerabilities via updates issued by hardware and software providers.[170] As specified in earlier sections, EMBs should implement technical controls such as encryption for data in transit and at rest. EMB IT departments should work with the legal department to tailor managerial and operational controls that derive from local legal frameworks and requirements, including ensure practices align with national and local laws around privacy protection and transparency obligations. EMBs should also establish – through managerial and operational controls – business continuity and recovery plans to ensure a quick, post-incident return to normal operations and clear contingency actions during cybersecurity events. When conducting field registration with standalone voter lists, the use of paper forms, in addition to direct field data entry, can serve as a hardcopy database backup in the event of data loss.

DRAFT

8. Candidate Registration Process

Overview and main uses of technology: Many countries have deployed technology solutions at the constituency level to capture and manage candidate registration and nomination processes, and use web-based applications for submitting relevant paperwork. Such systems collect and track party- and candidate-related information, storing personal details in various databases. This includes information such as tax identification numbers, biometric data, addresses, personal details such as birthdates, spousal information, criminal records, and sometimes financial data or returns. In some countries, candidates need to provide a list of supporters among eligible voters.

Although some of this information may be appropriate to disclose in the public domain for the sake of transparency, other data may be targets of malinformation, manipulation, or identity theft. As such, categories of data should be clearly delineated by the EMB and sensitive data should be protected.

Risk discussion: Risk arises if adequate security, such as end-to-end encryption, is not utilized. A threat actor might compromise and change data to either disqualify contestants that have a legitimate ground to stand, or artificially allow contestants that do not. This can lead to election postponement, annulment or rerun, and, in some cases, electoral violence. There is also risk

[169] Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388.

[170] Patch management is the process of distributing and applying updates to software. In this context, we are mostly concerned about security patches that aims to correct errors and fix vulnerabilities in the software. Security vulnerabilities are identified all the time, hence patch management should be a continuous process.

that this personal information may become a target for various malign actors seeking to steal information for political purpose or financial gain. Where electronic registration mechanisms are used, the information that is printed on election ballots is often derived from the registration system. Ballot errors (or manipulations) can lend prima facie grounds for election annulment, hence making for an attractive cyber target.

Mitigation strategies: To mitigate these threats, EMBs should implement the same sorts of controls discussed above that ensure network protection and encryption. Here, too, EMBs are advised to implement a system of least privilege to control access to these systems and clear criteria for when access is allowed. Efficient and immutable audit trails should be established so that any change can be traced back to individual users utilizing both operational and technical controls. EMBs should ensure that the management of candidate registration is compliant with the laws and regulations of the country with regards to protecting personal data.

9. Strategic communications

Overview and main uses of technology: EMBs increasingly rely on institutional websites and social media to communicate with stakeholders. Modern technology allows EMBs to engage with key audiences regarding activities, policies, legal and regulatory requirements, important electoral deadlines and voter education messages. These sorts of communications can support the mission of the EMB, improve the EMB's brand, and increase transparency.

DRAFT

One of the most controversial actions EMBs can undertake is introducing new technology without an extensive communication and awareness campaign to inform stakeholders. Procurement and operationalization of new technology should automatically trigger consideration about residual cyber risk and the roll-out should be accompanied by a well-conceived communication plan. EMB communication should avoid overselling the cyber-resilience of new technology, and instead emphasize the full array of mitigating measures and contingencies the EMB will undertake to assure the electorate and political stakeholders that the integrity of an election can be verified and upheld, even if a successful cyber attack occurs. EMBs might consider publicly communicating any cybersecurity testing it conducts on new technology.

Risk discussion: Compromised websites or social media accounts are a major risk for an EMB. Foreign or domestic state or non-state actors or independent hacking groups can damage the reputation of an EMB, even if the technical sophistication of the attack is minimal (such as website vandalism). Websites can be breached due to poor cyber hygiene (such as password and account protection practices), lack of patch management or poor third-party cybersecurity practices. While social accounts are critical tools to communicate with the public, poorly secured accounts and users lacking the knowledge and skills to identify and avoid social engineering attacks both create risks.

Mitigation strategies: The protection of privileged accounts is paramount to securing the online communication tools of EMBs; they must use strong passwords and multi-factor authentication. Users should be trained to identify phishing and other social engineering techniques, and they should have different devices for different accounts when possible, to prevent compromise of

multiple communication channels. Alternative communication plans should be prepared and tested well in advance, and should include media, civil society organizations and political parties as partners in such planning and preparation. These considerations should be folded into the defined control set used within any implemented cybersecurity risk management program, likely falling within more traditional business continuity planning activities.

10. Voter information and education

Overview and main uses of technology: The provision of voter information and education is often a continuous process occurring throughout all three phases of the electoral cycle. Voter awareness of election-related issues ensures voters know when, where, why and how to vote. This bolsters voter confidence in the electoral process and helps voters make an informed choice.

Risk discussion: Cybersecurity threats that may impact voter information and education efforts include denial of service attacks, which temporarily cut off public access to official sources of information about the election. Additional threats are posed by disinformation campaigns, which can target audiences by compromising or taking over official electoral social media and email accounts, and websites.[171] Disinformation campaigns can also reach the public through creation of social media and email accounts and websites that are intended to mimic official sources of information on elections.[172] These campaigns may undermine trust in an EMB or an entire electoral process. Disinformation can also seek to sow confusion about the election date or early voting periods, hours and locations, as well as about what types of identification are required to cast a ballot. Social media can also be abused to spread disinformation, such as reports or commentary distorting wait times or access at certain polling locations. Other targets of disinformation include voter registration dates and requirements, as well as the disenfranchisement of currently or previously incarcerated persons, tax enforcement linked to voter registration, and qualifications and procedures for absentee voting. Facebook seeks to flag and/or remove voter disinformation, and to proactively provide voters with correct information.[173]

DRAFT

Mitigation strategies: Legal frameworks can help mitigate some technological risks if local laws take into account such disinformation and enable enforcement activities. Strong strategic and crisis communication plans and cyber hygiene awareness are effective and necessary. EMBs should establish contingencies, redundancies, and mitigation mechanisms to ensure the continuous availability of services amid a breach by establishing pertinent controls within the

---

[171] In Cambodia in 2017 for example, the Facebook account for the Spokesman of the National Election Commission (NEC) was hacked and controlled by outside actors "for weeks," preventing accurate flow of information between the NEC, media and public. See https://www.phnompenhpost.com/national/nec-facebook-hack-investigated.

[172] In Georgia, for instance, a malicious actor set up a mock Facebook account named 'We are the Real CEC,' which mimicked the EMB's own Facebook page. This mock account was used to release false information (including a decree purportedly issued by the commissioner regarding election observers) and the content was reposted several times by other political actors.. See https://isfed.ge/eng/sotsialuri-mediis-monitoringi/manipulatsiuri-kampania-Facebook-ze-saarchevno-protsesebtan-dakavshirebit and https://factcheck.ge/en/story/39991-fabricated-image-of-the-cec-chairperson-s-decree-is-disseminated-through-social-networks.

[173] https://www.facebook.com/votinginformationcenter/

larger risk management plan. For instance, EMBs should plan for public-facing resources to be mirrored on a separate provider's system so that those resources can be quickly re-deployed in the case of compromise or availability issues. EMBs should also maintain relationships with social media platforms at the management level, to more effectively detect and counter disinformation operations.

B. Election Period

1. Voting process

Overview and main uses of technology: On Election Day, a variety of technologies may be used in polling stations for the process of voting, including electronic or biometric voter authentication to confirm registration and/or identify, direct recording electronic (DRE) voting machines, optical scanners, or ballot marking devices (BMD). Internet and absentee voting options are also part of this category and, as non-supervised voting methods with a potentially high number of technological components, also have a large exposure to various cybersecurity risks.[174]

Risk discussion: Cyber security risks include physical hardware and software manipulation. DRE have been shown to be vulnerable to various types of potential attacks, including man-in-the-middle attacks,[175] which seek to change information or votes.[176] These have been proven successful in controlled attempts both within the United States and the Netherlands, and to some extent, their success has also led to a significant adjustment or roll-back of this technology in these and other countries. The danger for electronic voting machine (EVM)~~EVM~~ manipulations does not only stem from the machine's software, but also the hardware. Supply-chain risk management has become a major concern following a recent increase in globally-reaching attacks.[177] If a threat actor can gain access to an EVM while it is being transported or assembled, for instance, there are several ways the machine may be altered to facilitate vote manipulation. A device could be inserted to take control of the unit, a chip that records the votes could be replaced with a fraudulent or malicious chip, or the software could be

DRAFT

[174] Applegate, Meredith, Thomas Chanussot and Vladlen Basysty. (2020). IFES. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. https://www.ifes.org/publications/considerations-internet-voting-overview-electoral-decision-makers.

[175] In cryptography and computer security, a man-in-the-middle, monster-in-the-middle,[1][2] machine-in-the-middle, monkey-in-the-middle (MITM) or person-in-the-middle (PITM) attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. See U.S. Department of Commerce, National Institute of Standards and Technology. Computer Security Resource Center: Man-in-the-Middle Attack. Accessed 21 Oct 2021. https://csrc.nist.gov/glossary/term/man_in_the_middle_attack#:~:text=Definition(s)%3A,involved%20in%20a%20communication%20association.

[176] https://arstechnica.com/information-technology/2011/09/diebold-voting-machines-vulnerable-to-remote-tampering-via-man-in-the-middle-attack/; and https://www.securitynewspaper.com/2017/07/31/def-con-voting-village-hackers-easily-pwned-us-voting-machines/

[177] In 2020, multiple government agencies and private companies (up to 18,000 clients in total) were compromised by an attack on the SolarWinds IT infrastructure company. In 2021, several companies were compromised by an attack on Microsoft Exchange Server.

compromised before it is installed in the EVM to alter votes after they are entered but before they are recorded.

Remote access to internet-basedfacing voter verification systems, sometimes using biometric functionalities, is used to prevent multiple voting and facilitate absentee voting, presenting a risk of voter suppression if penetrated. There have been few reported cases where these systems cause polling delays and queues due to denial of services attacks, but there is growing concern about the potential impact of such attacks.[178]

Mitigation strategies: To effectively combat threats to electronic voting, EMBs should implement controls that specify hardware- or firmware- level security settings that will help prevent manipulation. To mitigate third-party risk, EMBs should establish chains of custody, hardware inspections and efficient control of software and firmware hashes.[179] External interfaces such as USB ports should be disabled if not in use; full disk encryption hardware such as laptops and voting machines should be mandated and utilized; and physical security measures such as locks should be employed to prevent possible manipulation or theft of equipment. If possible under the contractual and legal agreement with the vendor, EMBs should consider security testing by independent parties, either through code and hardware inspections, penetration testing or other evaluations.

The use of VVPAT, along with transparent and inclusive audit procedures, is considered an established good practice, and is increasingly recommended by election observers and technical assistance providers. EMBs should also advocate for developing contingency plans within legal frameworks that address the possibility of compromised electronic voting technology. The operationalization of paper ballot-based contingency plans can be extremely time-consuming and costly. Therefore, postponement and rerun may offer more affordable options in case of localized cyber attacks on limited numbers of EVMs. Holding extra voting machines in reserve in case there is need for a replacement might also allow salvage an election in which a limited number of EVMs are compromised by cyber attack. Where VVPAT are available, legal frameworks must elaborate parallel procedures for counting and aggregated paper ballot receipts. This is discussed further in the counting section below.

DRAFT

2. Counting at the polling-station level

Overview and main uses of technology: Depending on a country's legal framework, the counting process may either take place directly after voting in individual polling stations, or at counting centers. A variety of technologies may be employed at this stage, including: scanners

[178] Although not a cyber-attack, a DOS impacted the Florida voter registration system https://apnews.com/article/election-2020-tallahassee-florida-elections-ron-desantis-8c986dbc04f5e5205fdcacfaa637b2af

[179] A hash is a function that can be used to calculate a unique digital fingerprint for the data. In this context, a hash value would be provided by the vendor when delivering the software or hardware, the EMB would calculate a new hash value for the software and hardware after it is receive. If the hash values are different, it can indicate the device has been tampered with during transmission or transport.

to ~~capture~~ process and tally voter choices on paper ballots; electronic machines that print ballot receipts that voters can check before they cast their ballot; and DRE machines that count votes without a paper record, or sometimes with a QR code that voters can check. If any vulnerabilities are exploited at this stage of the process, it can lead to questions about the integrity of electoral results and fundamentally undermine public confidence.

Risk discussion: The cybersecurity risks associated with the counting process include manipulation of hardware or software (by trusted or untrusted actors) to modify results. In several proof of concept demonstrations, ballot scanners have been exploited to modify the results of an election while leaving virtually no detectable trace of fraud.[180] The recent compromise of the software provider SolarWinds displayed how mundane software tools and the application of updates can be a vector for sophisticated attack.[181] Hardware and software utilized at polling stations, even if~~despite~~ relying on bespoke solutions, may still be exposed to threats emanating from determined adversaries that have infiltrated the supply chain of supporting or secondary infrastructure.

Mitigation strategies: All ICT devices present or used in the counting process should be *hardened* – the process of securing a server or computer system by minimizing the attack surface. Hardening includes both physical and software measures to prevent unauthorized access and manipulation. When EMBs purchase equipment, appropriate security tests should be utilized to define what hardening procedures should be applied to systems beyond the manufacturer's configuration. These procedures should be maintained and updated as appropriate as part the holistic risk management program.[182] As covered earlier, EMBs should obtain software and firmware hashes from manufacturers to ensure that devices and software have not been altered and that they are verifiably genuine. All devices should be certified before use. ICT devices should all use universal BIOS/UEFI security settings to prevent manipulation and tampering.[183] When not in use, all USB ports, WIFI and Bluetooth should be disabled. Ideally, the ICT systems used for the counting process will be housed in an enclosed case and have full disk encryption enabled.[184] EMBs should establish and maintain a proper chain of custody for transporting and storing the equipment. Tabulation audits are also integral to the mitigation strategy for lapses introduced during the counting process, as discussed in greater depth in the literature review, legal framework and results transmission sections of this report.

DRAFT

---

[180] https://www.springerprofessional.de/en/unclearballot-automated-ballot-image-manipulation/17199860

[181] `https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

[182] https://www.trentonsystems.com/blog/system-hardening-overview#:~:text=System%20hardening%20is%20the%20process,vulnerability%2C%20and%20potential%20attack%20vectors.

[183] Wilkins, R., & Richardson, B. (2013, September). UEFI secure boot in modern computer security solutions. In UEFI forum.

[184] Full disk encryption is a cryptographic method that applies encryption to the entire hard drive including data, files, the operating system and software programs. See https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html

11. Results transmission, tabulation and reporting

Overview and main uses of technology: As with counting, tabulation can take place at either the polling station level or at counting centers, depending on the law in place. It is important that results be demonstrably controlled to prevent questions of integrity or accuracy at each step through transmission and consolidation of results at central locations where results are certified. Multiple mechanisms have been used for the transmission of preliminary results to the higher-level commission, or sometimes directly to the central level, using Short Message Service (SMS) which is inherently unsecure; mobile phone reporting applications (including typed results and scans of paper forms); voice machine with transcription; or scanning digital pen with automated transmission. Various legal frameworks designate the electronic or the paper record as the legally valid record. Physically observable recounts, however, can only be conducted with paper records, whereby errors or manipulation in mobile transmission can be detected and corrected ex post. DREs, electronic machines, or scanners can also transmit results remotely to various levels of the EMB and are, therefore, also susceptible to possible attack.

Risk discussion: Attacks on results transmission and tabulation systems are a common tactics for actors seeking to undermine trust in elections. Such attacks may seek to alter vote counts or create public confusion and doubt about the integrity of an election's outcome. DDoS (distributed denial of service) attacks may also be staged at this phase of an election - preventing public access to results sites by overloading it with requests originating from a botnet.[185] Along with attacks on elections systems and websites, disinformation campaigns post a major threat in the post-election period. Release of false information about preliminary and final vote counts may seek to create doubt about the validity of election results, or to elevate social tension and strife.

DRAFT

One of the most prominent examples of this kind of attack occurred in Ukraine during the 2014 presidential election following the country's Revolution of Dignity and the subsequent invasion of Donbas by forces supported by the Russian Federation. On election night, a Moscow TV station, RT1, broadcast an election results website purporting to be that of the Ukrainian Central Election Commission (CEC) that showed the election was won by a minor pro-Russian, candidate. This hack into their website was discovered and quickly addressed by the CEC. As the data underlying it was not connected to the website, the CEC was able to restore the correct results on their website and fix the vulnerability. The incident, however, brought into sharp relief the damage that could have been done to the integrity of a pivotal election had the attack not been detected in time.

In 2018, Iraq began using ballot scanners that were expected to transmit results through the mobile phone network. The results of those ballot scanners that were used outside mobile phone coverage areas were loaded on USB memory sticks that were physically transported to regional results centers. Several such USB devices were reportedly intercepted and

[185] A botnet is a network or collection of compromised computers or hosts that are connected to the Internet. A compromised computer is controlled by an adversary to launch large scale attacks against target websites or infrastructure. See https://www.techopedia.com/definition/27201/zombie-network#:~:text=A%20zombie%20network%20is%20a,also%20known%20as%20a%20botnet.

manipulated. The results data was changed, so that it no longer aligned with the scanned ballots in the ballot box.[186]

Mitigation strategies: Wi-Fi functionality and Bluetooth should be disabled when not in use and controlled through use of standardized and managed hardware and software configuration policies. Hardware should be procured with requirements to limit functionality to only the necessary components.[187] As with the IT infrastructure discussed in earlier sections, end-to-end encryption must be used to ensure integrity of the data in transit and at rest. Proper cryptographic methods must be used to authenticate clients (for the data entry of results) and servers (to the centralization). Further, EMBs should use dedicated, offline, and/or encrypted infrastructure, as for instance the Venezuelan EMB does through the national phone company.

As discussed earlier in this paper, tabulation audits – including both fixed percentage and risk-limiting audits – are an important mechanism for ensuring the credibility and trustworthiness of technology-driven count and results processes.[188] As IFES has noted previously, such audits fundamentally require verifiable paper records of the intent of voters – to ensure an independent record of the votes cast to assess the accuracy of a tabulation system's results – making them of little value for the relatively small number of jurisdictions globally that use DREs without a paper trail. Some DREs produce a paper receipt that can be used as part of the audit trail, though this premise has been controversial. In India, for example, the Supreme Court ruled that all voting machines must be equipped with printers to provide voter- verifiable paper audit trails (VVPAT) to allow each voter to verify that his or her intended selections are correctly printed on a paper record, which is collected in a separate container called the VVPAT box."[189]

DRAFT

Such audits are also inherently limited in their ability to detect errors or incursions occurring in the voting system prior to the initial count. As Verified Voting has noted about risk-limiting audits in particular, "[they] are one piece of the larger ecosystem of evidence-based elections that depend upon a trustworthy record to give confidence to election outcomes. ... They do not tell us whether the voting system has been hacked. They do not and cannot determine whether voters actually verified their ballots. But they can detect and correct tabulation errors that could alter election outcomes..."[190]

Complementary procedures and compliance checks are needed that ensure that the paper and electronic records used in a tabulation audit are fully secured, including poll book accounting to compare the number of voters with ballots cast; ballot accounting to reconcile the number of ballots distributed with the number of ballots cast and the number of blank or spoiled ballots

---

186 EUEEM Final Report Iraq, 2018

187 Xie, T., Tu, G. H., Yin, B., Li, C. Y., Peng, C., Zhang, M., ... & Liu, X. (2020). The Untold Secrets of WiFi-Calling Services: Vulnerabilities, Attacks, and Countermeasures. IEEE Transactions on Mobile Computing.

188 See https://www.ifes.org/sites/default/files/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf

189 Mohanty, V., Akinyokun, N., Conway, A., Culnane, C., Stark, P. B. & Teague, V. (2019). Auditing Indian Elections. p. 2. Retrieved from: https://arxiv.org/pdf/1901.03108.pdf.

190 Verified Voting. (2019). The Role Of Risk-Limiting Audits In Evidence-Based Elections. Retrieved from: https://verifiedvoting.org/the-role-of-risk-limiting-audits-in-evidence-based-elections/

returned; reconciliation of votes to check mathematical accuracy of tabulation forms; chain of custody checks to review signature logs and ensure custody of all secure election materials; and security checks to ensure that ballots and boxes have been protected with tamper- evident seals and other security features.[191] Proper chain of custody in particular "is a crucial component of investigation and dispute resolution, more generally, as adjudication decisions may be affected by the quality of the physical evidence supporting a complaint."[192] Compliance checks are also valuable in the event of a court challenge against the results.

It is similarly important that the EMB makes every effort to centrally retain a full set of the official paper-based results forms for verification of results, or recounts, should a court of law order one or if the legal framework contains triggers for one. In 2017, the Kenyan EMB relied so heavily on its electronic results transmission system, KIEMS, that it neglected to centrally collect and verify the original signed paper results sheets before releasing results. In absence of a full record of all polling station results forms justifying the EMB's national results announcement, the Supreme Court (constrained by a 2-week deliberation period) saw no other option than to annul the election nationwide.

C. Post-Election Period

1. Electoral dispute resolution process

Overview and main uses of technology: Effective resolution of electoral complaints is essential to the integrity and legitimacy of an election. EMBs increasingly accept complaints through online channels, facilitating the lodging of grievances, but also allowing new ways for malicious actors to tamper with or to disable online complaints system. Some online portals allow uploading of electronic evidence, such as documents, photos and video. Both EMBs and EDR tribunals also increasingly rely on electronic case management systems, which can be accessible to the public in order to allow tracking of complaints through the adjudication stages.[193] Many EMBs and EDR tribunals also upload decisions on their homepages, and some tribunals have begun holding hearings remotely because of the Covid-19 pandemic.

DRAFT

Risk discussion: Election complaints portals can be overloaded with frivolous and unsubstantiated complaints by malicious actors, and could suffer from attacks impacting the availability and integrity of the data collected and stored. In many countries, judiciaries play a vital role in the resolution of election claims. As such, institutional webpages of the court system can be as vulnerable to cyber attack as EMB webpages.

Complaints related to electronic votes or electronic transmission might require EDR tribunals to use external expertise to conduct cyber forensics in the event that inconsistencies are found or compromise of the system is suspected. The absence of reliable and trusted digital evidence[194]

---

[191] Shein, E. & Brown A. (2021). "Risk-Limiting Audits: A Guide for Global Use." IFES. https://www.ifes.org/publications/risk-limiting-audits-guide-global-use.

[192] Vickery, C. & Ellena, K. (2020). Election Investigations Guidebook. Retrieved from: https://www.ifes.org/publications/election-investigations-guidebook

[193] https://www.cartercenter.org/resources/pdfs/peace/democracy/des/edr-approach-paper.pdf

can lead to annulling the election. In 2017, the Kenyan EMB restricted judicial and political party access to the results management server, which had allegedly failed to receive results of more than a third of the districts. The court ruled that it could not ascertain whether the results management system had been breached or otherwise failed, and criticized the EMB for its management of election technology.

In the Democratic Republic of the Congo in 2018, the legal and regulatory framework neglected to establish evidentiary hierarchy between electronically transmitted results/EVM results printouts and handwritten/signed polling station results forms (meaning it was unclear which took legal precedent). The EMB never centralized or aggregated the hardcopy paper results chain, and the court declined to subpoena the electronic transmission chain, so it remains unclear whether the system was attacked, and if so, whether it withstood those attacks. The ultimate cybersecurity risk in this category would involve a successful cyber attack that deprived EDR tribunals from any actionable evidence to either validate or invalidate preliminary results, unless the EMB transmitted and centrally tabulated hard-copy results.

Another risk is around case file management systems, which should be maintained during all phases of the electoral cycle. However, these systems may lack vendor support, and may utilize outdated hardware and software -- complicating the process of securing them.

Individual judges can become victims of invasion of cyber privacy, in order to either discredit them, or to blackmail them into either confirming or overturning election results.

Finally, the judiciary may also be involved in investigating cyber-attacks against elections, and use of technology in such investigations and prosecutions might once again be targeted by cyber-attack to thwart efforts by law enforcement.

DRAFT

Mitigation strategies: Whether electronic case management systems are in place for election disputes or not, EMBs and courts should allow for paper-based submission of grievances, as well as publish their decisions in official journals and newspapers, in case electronic channels are compromised or disabled. Communications should be acknowledged, and receipts produced with unique identifiable code to trace the originals and associated timestamp of the communication. More importantly, the legal framework must clearly provide for the regulation of election technology, the legal primacy of a paper trail, and the ability for systems to be both secure and transparent. Finally, the law must give EDR courts the necessary mandate to investigate the integrity of election technology processes and outcomes through post-electoral audits (that are clearly regulated in advance), as well as through empower them – via experts -- to perform cyber-forensics of the results chain. Technical assistance providers can support EDR courts in developing tools and methodologies to meet such mandates.

12. Detecting, investigating and prosecuting cybercrime in elections

Overview and main uses of technology: Malicious activity involving a computer, computer network or a networked device to conduct a criminal act is known as a *cybercrime*. A range of

---

[194] Digital evidence, its definition and qualities are now very well define in both criminal and civil law contexts https://www.americanbar.org/products/inv/book/261961916/

cyber attacks, including hacking voter databases, tampering with voting machines, denial of service attacks or theft of data for information operations in elections could represent a cybercrime under national legal frameworks and the 2001 Budapest Convention.[195] While a major focus of governments is necessarily protecting networks from attack, this may not be a sufficient deterrent against future attack, and the detection, investigation and prosecution of cybercrime in elections remains important. When it comes to cyber attacks against elections, the Venice of Commission concludes that, "greater efforts need to be undertaken to prosecute such interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections."[196]

Risk discussion: Cyber attacks against elections have so far yielded few arrests. In 2020, a man was arrested for perpetrating distributed denial of service attacks against the website of a congressional candidate in California.[197] There are many challenges to detecting, investigating, and prosecuting cybercrime in elections. This includes challenges around jurisdiction, and the need for international legal cooperation where such crimes are cross-border. For example, the Russian Federation refuses to extradite its citizens to foreign states on cyber crime charges, and is not a signatory to the 2001 Budapest Convention. As a response, the European Union has placed targeted sanctions on the suspects.[198] The United States government made its first indictment against foreign election cyber attackers in 2018, but was not able to take custody of the 12 suspects.[199] A second challenge is anonymity, and the tension between detecting perpetrators of cyber-crime while protecting privacy rights. Finally, evidence in cybercrime cases can be a challenge, as it is often fragile and easily destroyed. It can also be difficult to maintain a chain of custody. All these challenges put the investigation and prosecution of cybercrime at risk.

DRAFT

Mitigation strategies: In 2020, IFES issued the Election Investigations Guidebook—Standards, Techniques and Resources for Investigating Disputes in Elections (STRIDE), which advises EMBs and investigators on principles for detecting and combatting electoral offenses, in line with international standards.[200] It is imperative that EMBs and investigators are able to secure electronic evidence, and where necessary cooperate with a range of domestic agencies and international law enforcement personnel under the Budapest Convention to identify and prosecute offenders (and to secure evidence that may be in other jurisdictions). There may also be a need to cooperate with service providers on both protecting and accessing evidence. In 2019, the United Nations Office on Drugs and Crime (UNODC) department on cyber-crime published its Training Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns & Warfare in Cyberspace, Information Warfare, Disinformation & Electoral Fraud. [201] In the spirit

---

[195] https://www.coe.int/en/web/cybercrime/-/cybercrime-in-elections

[196] https://rm.coe.int/electoral-dispute-resolution/16809f0007 page 107

[197] https://www.justice.gov/usao-cdca/pr/santa-monica-man-arrested-federal-charges-staging-cyberattacks-computer-system

[198] https://www.securityweek.com/eu-slaps-sanctions-2-russians-over-germany-cyberattack

[199] https://www.bbc.com/news/world-us-canada-44825345

[200] https://www.ifes.org/sites/default/files/ifes_election_investigations_guidebook_december_2020.pdf

of the Budapest Convention, EMBs may also consider initiating peer platforms for information and good practice sharing, as well as international emergency hotlines in the realm of detecting and investigating cyber-attacks on elections.

Similar to the CSO context, high profile political targets will not be protected by basic cyber-hygiene practices. As demonstrated by the Pegasus leak,[202] some countries will use surveillance tools to monitor activities of political opposition. High profile political targets could call upon specialized agencies to secure their devices, otherwise they should consider them compromised. The objectives of the national or foreign state targeting high profile targets will usually be discrediting or acquiring information that can be used for blackmail.

VI. Conclusions

The analysis in this report illustrates the way electronic information systems are heavily utilized across the electoral cycle. In cybersecurity terms, that infrastructure represents an expansive "attack surface" that can be threatened and exploited by foreign or domestic adversaries who intend to disrupt the electoral process.

While some established democracies have rolled back their use of technology for specific aspects of election administration, overall, the further digitization of the electoral process will likely only increase. In fact, the COVID-19 pandemic further accelerated the pace of digitization. In this context of tension between offering more services online to stakeholders and securing an increasingly adversarial environment, electoral stakeholders and democracy donors need to consider the cybersecurity risks associated with technological components, whether it is directly or indirectly related to the electoral process. Doing so in a piecemeal or ad hoc manner may not be sustainable, or sufficiently effective to counter current and future integrity threats. In this regard, lessons drawn from the larger cybersecurity industry – which emphasizes holistic management of cybersecurity – are applicable to the electoral space and should be embraced by the election community. Cybersecurity must be an ongoing process of risk management rather than a static requirement; mature cybersecurity programs are adaptable and continuously recognize threats and curate security mechanisms to address those threats through controls, vulnerability management, and continuous evaluation.

DRAFT

We recognize, however, that many EMBs may not currently be sufficiently resourced or positioned to enact such mature cybersecurity programs. The risk management frameworks use by governments and industry need to be adapted for the electoral space and further work must be done to tailor them to local contexts. While there has been a great deal published recently to advance thinking about the intersection of cybersecurity and electoral operations globally, there is still much more that needs to be done. At the national level, some countries are saddled with laws and regulations that effectively prevent electoral stakeholders from addressing emerging issues of the digital age. These issues are myriad and include assigning responsibility for protection of electoral infrastructure, standardizing security requirements,

---

[201] https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html

[202] https://cdn.occrp.org/projects/project-p/#/professions/politician

coordinating the flow of information across various stakeholders, and securing information against misuse while also anticipating and planning for response and resiliency. Cybersecurity must be considered at every stage of the electoral process, which is currently not the case in many countries. These considerations include implementing fundamental managerial controls such as policies that ensure procurement of secure ICT-related solutions from reputable vendors. They also include operational controls of ICT-equipment and databases executed by employees, volunteers, and other related users that minimize risk. Finally, these considerations include how to best implement technical controls such as automated cyber defenses to help ensure security throughout the electoral cycle. Good practices are emerging and will need to be codified and circulated for the electoral community to further institutionalize adoption at national and local levels.

Safeguarding the practice of elections in the cyber era is not simple, as the electoral process varies significantly globally, as do the threat profiles. The institutions and stakeholders involved in elections often control elements of the information technology infrastructure independently; therefore, any compromise of confidentiality, integrity, and/or availability may have systemic effects across the electoral process that could undermine the entire election. There are practical steps EMBs, political parties, and civil society organizations, among others, can take to further mature election cybersecurity. While these practical steps begin with the education of users to exercise adequate cyber hygiene, they extend much further across all levels of electoral management. Incorporating modern security controls and practices will undoubtedly take time and resources while requiring further adaptation across democracies worldwide, each with their unique context and local intricacies.

DRAFT

2. Annex A: List of relevant publications or resources

A. International, Regional, and Domestic Standards

Brown, I., Marsden, C. T., and Lee, J. 2020. The Commonwealth. Cybersecurity for Elections: A Commonwealth Guide on Best Practice.

Catt, H., et al. 2014. International IDEA. Electoral Management Design, revised ed.

Council of Europe. 2017. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting.

Council of Europe. 2011. Certification of e-voting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards.

Council of Europe, Venice Commission. 2018. Draft Compilation of Venice Commission Opinions and Reports Concerning New Technologies in the Electoral Process.

European Commission. 2006. EC Methodological Guide on Electoral Assistance.

European Commission and United Nations Development Programme. 2010. Procurement Aspects of Introducing ICTs solutions in Electoral Processes.

European Union. 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

European Union. 2018. Compendium on Cyber Security of Election Technology.

Open Government Partnership. 2011. Open Government Declaration.

OSCE/ODIHR. 2013. Guidelines for Reviewing the Legal Framework for Elections, 2nd ed.

United Nations General Assembly. 1990. Guidelines for the Regulation of Computerized Data Files.

U.S. Election Assistance Commission. 2021. Voluntary Voting System Guidelines: Major Updates of the Voluntary Voting System Guidelines 2.0.

B. Practitioner Publications

Calkin, B. et al. 2018. Center for Internet Security. A Handbook for Elections Infrastructure Security.

Caufield, M. 2021. Verified Voting. The Price of Voting: Today's Voting Machine Marketplace.

DRAFT

Cortés, Edgardo et al. 2019. Brennan Center for Justice at New York University School of Law. Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials.

Ellena K., et al. 2018. IFES. Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies.

Goldsmith, B. 2011. IFES. Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies.

Goldsmith, B. and Ruthrauff H. 2013. IFES, NDI. Implementing and Overseeing Electronic Voting and Counting Technologies.

Holtved, O. 2011. IFES, USAID. Biometrics in Elections.

Miller, G., Perez, E., Sebes, J. E., Valente, S. 2020 (2nd ed.). OSET Institute. Critical Democracy Infrastructure Protecting American Elections in the Digital Age Threats, Vulnerabilities, and Countermeasures as a National Security Agenda.

McCormack, C. 2016. Atlantic Council. Democracy Rebooted: The Future of Technology in Elections.

Norden, Lawrence and Andrea Córdova McCadney. 2019. Brennan Center for Justice at New York University School of Law. Voting Machines at Risk: Where We Stand Today.

Pact, Inc. 2014. Mobile Technology Handbook.

Plunkett, D., Monsky, H., et al. 2017. Harvard Kennedy School, Belfer Center. Cybersecurity Campaign Playbook.

Rhodes, Jill and Robert S. Litt, Eds. 2017. ABA Book Publishing. The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition.

Shein, E. and Brown, A. 2021. IFES. Risk Limiting Audits.

Van Der Staark, S., and Wolf, P. 2019. International IDEA. Cybersecurity in Elections – Models of Interagency Collaboration.

Wolf, P., Alim, A., et al. 2017. International IDEA. Introducing Biometric Technology in Elections.

Wolf, P. et al. 2017. International IDEA. Introducing Biometric Technology in Elections.

World Wide Web Foundation. 2017. Open Data Barometer Global Report – Fourth Edition.

Yard, M. (Ed.) 2010. IFES. Direct Democracy: Progress and Pitfalls of Election Technology,

Yard, M. (Ed.) 2011. IFES. Civil and Voter Registries: Lessons Learned from Global Experiences. Civil and Voter Registries: Lessons Learned from Global Experiences. et al. 2018. Center for

DRAFT

Internet Security. A Handbook for Elections Infrastructure Security. Wolf, P. et al. 2017. International IDEA. Introducing Biometric Technology in Elections

C. Cybersecurity Instruments and Frameworks

Center for Internet Security. The 18 CIS Critical Security Controls.

European Agency for Cybersecurity. ENISA Risk Management /Risk Assessment Framework.

Gebremedhin Kassa. 2016. S. ISACA Journal (vol. 5). Information Systems Security Audit: An Ontological Framework.

Information Systems Audit and Control Association (ISACA). 2019. Control Objectives for Information Technology (COBIT).

International Organization for Standardization (ISO). ISO 31000 Risk Management.

International Organization for Standardization (ISO). ISO 27001 Information Security Management.

National Institute of Standards and Technology. 2018 (ver. 1.1, 3). Framework for Improving Critical Infrastructure Cybersecurity.

DRAFT

National Institute of Standards and Technology. 2018 (ver. 1.1). Cybersecurity Framework.

National Institute of Standards and Technology. 2018 (rev. 2). Special Publication 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

National Institute of Standards and Technology. 2020 (rev. 5). Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations.

National Institutue of Standards and Technology. 2021. NIST Interagency or Internal Report 8310 (Draft) Cybersecurity Framework Election Infrastructure Profile.

D. Election Observer Guidelines

Adams-Cohen, Nicholas J. et al. 2017. Caltech/MIT: Voting Technology Project (Working Paper No. 129). Election Monitoring Using Twitter.

Aldana, G., et al. Organization of American States, Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions.

Carter Center. 2012. Observing Electronic Voting.

OSCE/ODIHR. 2013. Handbook for the Observation of New Voting Technologies.

Pran, V and Merloe, P. 2007. NDI. Monitoring Electronic Technologies in Electoral Processes.

Wagner, Ben. 2020. The Political Quarterly (vol. 91, is. 4). Digital Election Observation: Regulatory Challenges around Legal Online Content.

E. Academic Literature

Gambhir, R. K., & Karsten, J. 2019. Brookings Institution. Why Paper Is Considered State-of-the-Art Voting Technology.

Norden, L., Cordova McCadney, A. 2019. Brennan Center for Justice at New York University School of Law. Voting Machines at Risk: Where We Stand Today.

Feldman, A., Halderman, J., Felten, E. 2007. Conference Paper: USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07). Security Analysis of the Diebold AccuVote-TS Voting Machine.

Balzarotti, D. et al. 2010. IEEE Transactions on Software Engineering (Vol. 36, No. 4). An Experience in Testing the Security of Real-World Electronic Voting Systems.

Wolchok, S., et al. 2010. Conference Paper: 17th ACM Conference on Computer and Communications Security. Security Analysis of India's Electronic Voting Machines.

Gonggrijp, R., & Hengeveld, W. J. 2007. Conference Paper: USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07). Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective.

National Democratic Institute. Accessed 2021. Re-evaluation of the Use of Electronic Voting in the Netherlands.

MIT Election Data + Science Lab. Accessed 2021. Voting Technology.

Berger, M., et al. 2018. Harvard Kennedy School, Belfer Center. The State and Local Election Cyber-Security Playbook.

Park, S., Specter, M., Narula, N., Rivest, L R. 2020. Journal of Cybersecurity (Vol 7, Iss 1). Going from Bad to Worse: From Internet Voting to Blockchain Voting.

Haines, T., Lewis, S. J., Pereira, O., Teague, V. 2020. Conference Paper: IEEE Symposium on Security and Privacy. How Not to Prove Your Election Outcome.

Springall, D., et al. 2014. Conference Paper: ACM SIGSAC Conference on Computer and Communications Security. Security Analysis of the Estonian Internet Voting System

Wolchok S., Wustrow E., Isabel D., Halderman J.A. 2012. Attacking the Washington, D.C. Internet Voting System. In Keromytis, A.D. (ed). 2012. Lecture Notes in Computer Sinance (Vol 7397) Financial Cryptography and Data Security. 2012. Lecture Notes in Computer Science (Vol 7397). (Springer: Berlin, Heidelberg).

DRAFT

Kshetri, N., & Voas, J. 2018. IEEE Software (Vol 35, Iss 4). Blockchain-Enabled E-Voting.

Specter, M. A., Koppel, J., & Weitzner, D. 2020. Conference Paper: 29th USENIX Security Symposium. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections.

Gaudry, P., & Golovnev, A. 2020. Conference Paper: International Conference on Financial Cryptography and Data Security. Breaking the Encryption Scheme of the Moscow Internet Voting System.

F. Jurisprudence

Odinga v. IEBC et al., (2017) (S.C.K) (Kenya).

Swamy v. Election Commission of India (SC) (2009) (India).

BVerfG, 2 BvC 3/07, 2 BvC 4/07, Mar. 3, 2009.

KHO:2209: 39 (Supreme Administrative Court of Finland)

Constitutional Judgment 3-4-1-13-05, Mar. 23, 2011, (SC) (Estonia).

Curling, et al. v. Raffensperger, et al., 403 F. Supp. 3d 1311 (N.D. Ga. 2019).

Tuggle, et al. v. Ala. Sec'y of State John Merrill, No. 1170216, May 18, 2018, (Ala.).

DRAFT

G. Other Reports

US Department of Justice, Office of the Deputy Attorney General. 2018. Report of the Attorney General's Cyber Digital Task Force.