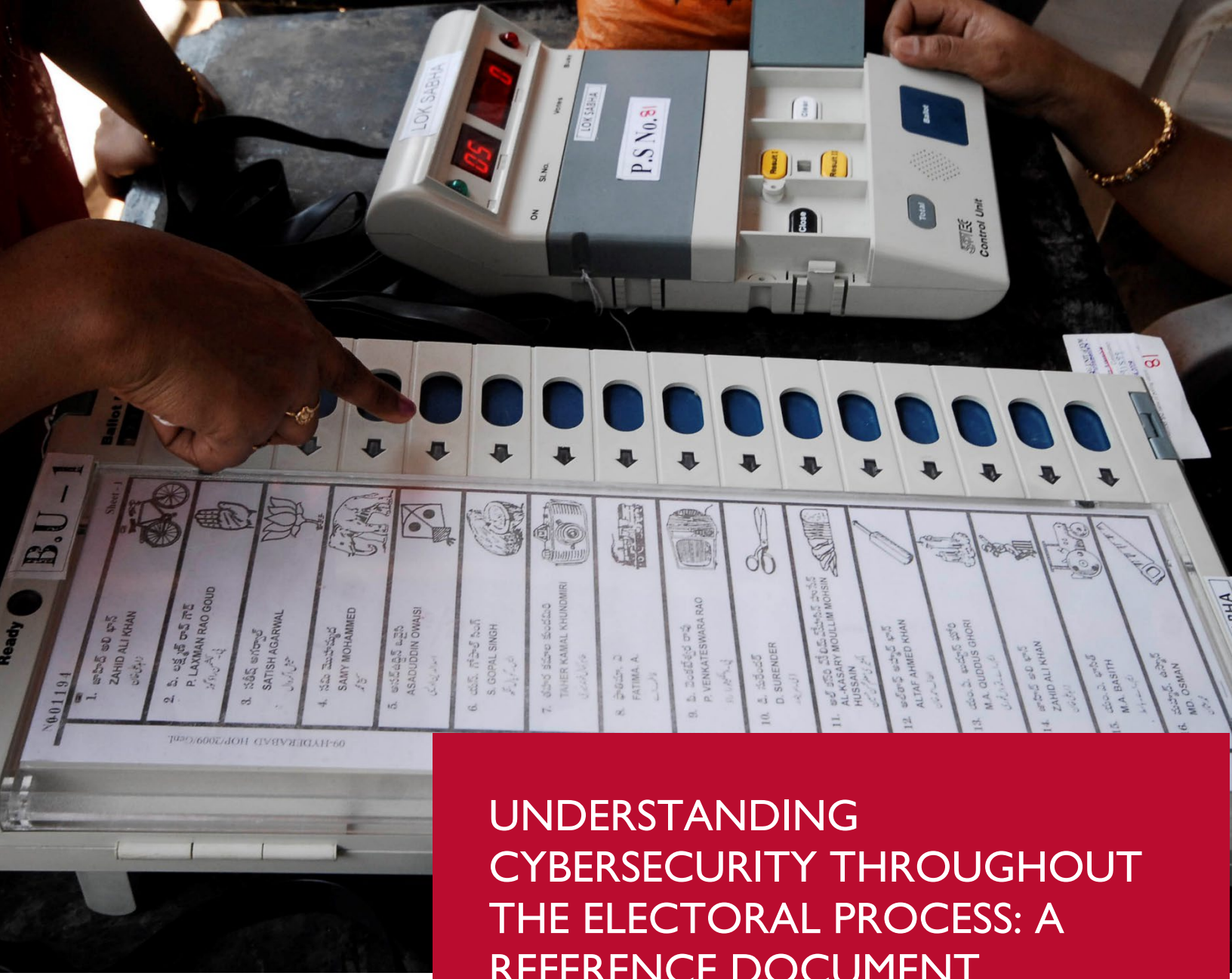

PHOTO © AP PHOTO/MAHESH KUMAR A. 2009

UNDERSTANDING CYBERSECURITY THROUGHOUT THE ELECTORAL PROCESS: A REFERENCE DOCUMENT

An Overview of Cyber Threats and Vulnerabilities in Elections

USAID FROM THE AMERICAN PEOPLE
DAI Shaping a more livable world.
International Foundation for Electoral Systems

Acknowledgements

This reference document was prepared by the International Foundation for Electoral Systems (IFES) Center for Applied Research & Learning in consultation with DAI and USAID's Center for Democracy, Human Rights and Governance (DRG Center). Dr. Tarun Chaudhary, Thomas Chanussot, and Dr. Manuel Wally were lead authors. The reference document benefited tremendously from contributions by Dr. Stephen Boyce, Dr. Beata Martin-Rozumiłowicz, Dr. Staffan Darnolf, Chelsea Dreher, Katherine Ellena, Brian Polk, Federico Roitman, Victoria Scott, Erica Shein, and Chad Vickery. The authors would also like to acknowledge Annie Styles for her immense help. The team is grateful to those individuals who reviewed various drafts and provided valuable insights

*Research and drafting were completed by the International Foundation for Electoral Systems, in cooperation with DAI

CONTENTS

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,[2] and can mitigate or prevent some types of election fraud.[3] 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 to address the potential for disruptive cyber attacks.[4]

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. Failure to address electoral cybersecurity risks can pose a critical threat to electoral integrity. Malign actors may attempt to manipulate elections directly, undermine public confidence in elections, or erode the legitimacy of elected representatives and bodies by exploiting vulnerabilities in electronic information processing and cyberspace. Such loss in trust and concerns about legitimacy could impede development initiatives and undermine effective and accountable governance.

As the number of election technology applications grows, elections have begun to attract the attention of a wider spectrum of threat actors. Cyberspace, despite all the societal benefit and economic value it has helped create, is also an arena of strategic competition and criminal activity. The electronic information systems in use across electoral processes are therefore important elements of critical national infrastructure that can be attacked. There are well known examples of cyber attacks focused 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.

Election managers should look to trends identified within the wider field of cybersecurity analysis to understand the types of attacks that can potentially impact systems falling under their purview. While denial of service attacks that overload infrastructure and other relatively unsophisticated attacks are still occurring, recent analysis has highlighted how a commoditized market for sophisticated tools and methods

---

[1] Goldsmith, B. and H. Ruthrauff. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. National Democratic Institute and International Foundation for Electoral Systems. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies, pp. 21-22; and National Democratic Institute. (n.d.). The Rationale for E-voting in Brazil. https://www.ndi.org/e-voting-guide/examples/the-rationale-for-e-voting-in-brazil.

[2] Human Systems Integration Division, Electronic Systems Laboratory, Georgia Tech Research Institute, Georgia Institute of Technology. (2012, July). Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment. https://www.nist.gov/system/files/documents/2017/05/09/GTRI-Appendix-A-Accessibility-of-Voting-Systems.pdf

[3] Somanathan, M. (2019, April 5). India's Electoral Democracy: How EVMs Curb Electoral Fraud. Brookings Institute. https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/

[4] The attacks on Ukraine in 2014 and the United States in 2016 are particularly illuminating. See, for instance, Martin-Rozumilowicz, B. and T. Chanussot (2019). "Cybersecurity and Electoral Integrity: The Case of Ukraine, 2014-Present." In Krimmer, R. et al (Eds). Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019: 1-4 October 2019, Lochau/Bregenz, Austria: Proceedings. https://www.zora.uzh.ch/id/eprint/175950/

has lowered barriers and allowed lesser resourced actors to purchase greater malicious effect.[5] Threat actors often also use methods of deception to trick users into clicking on malicious links or disclosing sensitive information like passwords in a practice called "phishing." Often nation-state actors will utilize their intelligence resources to target individuals using content tailored or engineered specifically for that person in the practice of spear-phishing. Once sensitive information is obtained, it can often be leveraged to compromise systems and establish a foothold within a network. That foothold can then be utilized for any number of purposes. Criminal elements may, for example, deploy software that encrypts data in financial extortion schemes.[6] Nation-states or other sophisticated actors may use such a foothold to execute further penetration of a network and exfiltrate sensitive and confidential information they can leverage for intelligence purposes.

The range of stakeholders that are being targeted with cyber attacks – and are working to prevent and respond to them – is also 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.

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

The purpose of this report is to help USAID Democracy, Human Rights, and Governance (DRG) staff and other relevant U.S. Government personnel to better understand the nature of electoral cybersecurity risks and threats in the contexts in which they work. Drawing on the fields of both electoral management and cybersecurity risk management, it provides an entry-level overview of electoral cybersecurity threats, vulnerabilities, threat actors, and mitigation measures across key aspects of the electoral process. It also outlines good practices that EMBs can leverage to mitigate and address cyber threats.

The report is designed to be useful to individuals that may not have prior cybersecurity knowledge. It focuses on the 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, 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 process 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)

[5] The Microsoft Digital Defense Report issued in October 2021 has recent trending data. See: Microsoft. (2021, October). Microsoft Digital Defense Report. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[6] The term ransomware is often used to describe this practice.

to establish mature cybersecurity postures to holistically recognize and manage the risks individually and collectively across the electoral process.

In particular, a review of recent trends indicates 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 election processes.

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. Therefore, it is important that the concern of cybersecurity be addressed holistically throughout electoral infrastructure. EMBs need to educate users of electronic information systems in proper cyber-hygiene. Policies and processes that inculcate and support cybersecurity good practice need to be put in place, and EMBs will need to invest in executive oversight, advocacy, and management of cybersecurity through professionalized and dedicated workforce roles.

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 election management body (EMB). The EMB has multiple responsibilities, including maintaining integrity throughout the planning process, carrying out elections, and finalizing results.[7] 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.[8] 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.

OFTEN OBSERVED CYBER ATTACKS

DENIAL OF SERVICE	PHISHING	RANSOMWARE
Attackers make multiple requests that overload and cause a website or online resource to fail. Often attackers can purchase malicious services that utilize compromised computers connected to the internet under remote command and control that can be directed to make such requests. These networks are called "botnets" and perform a "distributed denial of service" attack.	Attackers use methods of deception to trick unsuspected users into clicking on malicious links that trigger the download of software that can compromise their system or deceive users into providing passwords that can then be utilized to compromise accounts.	Attackers compromise a network and encrypt data. The attackers may then contact a victim promising to send a decryption key in exchange for money.

[7] For a comprehensive overview of the various institutional arrangements associated with the management of democratic elections, see: Catt, Helena et al. (2014, September). *Electoral Management Design, Revised Edition.* International Institute for Democracy and Electoral Assistance. https://www.idea.int/sites/default/files/publications/electoral-management-design-2014.pdf

[8] Please see the National Institute for Standards and Technology's (NIST) Glossary for definitions. National Institute for Standards and Technology. (n.d.). *Glossary*. https://csrc.nist.gov/glossary/term/cybersecurity

Elections all over the world have been 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 – 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 systems – 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 provides an overview of the more practical threats to elections and outlines the concept of cybersecurity as a risk management process that should be adopted by EMBs. The paper begins with an overview of technology adoption and cybersecurity threats in elections and a brief literature review of the existing body of work that informs electoral cybersecurity policy and practice.

Next, the paper discusses the primary actors posing cyber threats to election technology. It then applies the key cybersecurity concepts of risk management and security control mechanisms to the electoral process using a risk-based approach with a focus on mitigation strategies for election management bodies. The penultimate section considers the importance of multi-stakeholder coordination and outlines cyber risks for two additional stakeholder groups: political parties and civil society organizations.

The paper concludes with a discussion of areas where further analysis and guidance is needed to strengthen the cybersecurity postures of electoral management bodies.

---

[9] Marañon, A. (2021, May 28). *How Have Information Operations Affected the Integrity of Democratic Elections in Latin America?* Lawfare. https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democratic-elections-latin-america

[10] Allen, N. and N. van der Waag-Cowling. (2021, July 15). *How African States Can Tackle State-Backed Cyber Threats*. Brookings Institute. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

[11] Lim, Y. (2020, November 22). *Election Cyber Threats in the Asia-Pacific Region*. Mandiant. https://www.fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html

[12] Galloway, Anthony. (2020, October 28). *Cyber Attacks on Elections Growing Amid Concern for Australia's Political Parties*. Sydney Morning Herald. 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. and Fetterolf, J. (2019, January 9). *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] TeleSURtv.net. (2021, August 2). TSE de Brasil Respalda Sistema de Voto Electrónico. https://www.telesurtv.net/news/brasil-tse-respalda-sistema-voto-electronico-20210802-0026.html

II. CYBERSECURITY IN ELECTIONS: A BRIEF HISTORY AND OVERVIEW OF THE LITERATURE

Traditional, manual voting and hand-counting paper ballots have 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 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 increased 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, for instance, put the use of electronic voting machines (EVMs) on hold months before their planned use in nationwide elections in 2004[19] due to security vulnerabilities and because they did not produce a paper trail. The government ultimately decided to dispose of their EVMs in 2009.[20] In Finland, EVMs were piloted in three municipalities in 2008 (traditional paper balloting was also available at each location).[21] Ultimately the municipal election votes were annulled by the Supreme Administrative Court due to dissemination of flawed instructions on EVM use, and flaws in the EVM-voter interface (in which the system failed to inform voters that their ballots had not been successfully cast).[22] The Finnish government subsequently decided to stop using this technology.

---

[15] International Foundation for Electoral Systems. (2014, November 20). *Electronic Voting Machines Pakistan Factsheet*. 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 and Democratic Values*, 73 Fordham L. Rev. p. 1719. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4064&context=flr

[16] National Democratic Institute, *The Rationale for E-voting in Brazil.*

[17] Georgia Institute of Technology, *Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment.*

[18] Somanathan, *India's Electoral Democracy: How EVMs Curb Electoral Fraud.*

[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. (n.d.). *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/

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 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] Since 2003, instances of People's Republic of China (PRC) hackers (often associated with various state ministries) infiltrating U.S. networks to acquire national security information or intellectual property have been documented.[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 Kremlin.[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 Ukraine's 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 addition, in November of 2021 the U.S. Department of Justice announced charges against two Iranian nationals for interference with the 2020 Presidential election. The charges included obtaining "…confidential United States voter information from at least one state election website."[29] Earlier in 2021, the German election administration was also targeted by cyber attacks.[30] The same week

---

[23] Bundesverfassungsgericht. (2009). Judgment of 3 March 2009 - 2 BvC 3/07. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

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

[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, "Cybersecurity and Electoral Integrity."

[29] United States Attorney's Office, Southern District of New York, United States Department of Justice. (2021, November 18). *U.S. Attorney Announces Charges Against Two Iranian Nationals for Cyber-Enabled Disinformation And Threat Campaign Designed To Interfere With The 2020 U.S. Presidential Election*. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-two-iranian-nationals-cyber-enabled

[30] AFP. (2021, September 17). *German Election Authority Confirms Likely Cyber Attack.* Security Week. https://www.securityweek.com/german-election-authority-confirms-likely-cyber-attack

the German election administration detected these attacks, the Russian Central Election Commission (CEC) reported attacks during its three-day voting period.[31]

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 principles, guidelines and legal frameworks; good practice publications from practitioner and election observation organizations; cybersecurity instruments and frameworks; 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] This review is not comprehensive, but is intended to illustrate the range of sources for information.

A. INTERNATIONAL, REGIONAL AND DOMESTIC GUIDANCE FOR CYBERSECURITY IN ELECTIONS

The first source for policy and good practice in cybersecurity in elections is guidance and, in some cases, legal frameworks proffered by international and regional organizations and domestic governing authorities. For ease of review, this section has been divided into two categories that cover the main types of frameworks relevant to the electoral process: election technology and cybersecurity; and open data, transparency and privacy in the digital space.

1. ELECTION TECHNOLOGY AND CYBERSECURITY THREATS

Standards for the introduction of technology in voting or vote-counting processes have been developed on the regional or domestic level. 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."[33] 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."[34]

Some countries establish their own voluntary guidelines around election technology. 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 guidelines as obligatory.[35] Certification of election technologies has also

[31] News Room. (2021, September 20). *Russia. 3 Cyber Attacks Targeting the Elections in their First Day*. Eastern Herald. https://www.easternherald.com/2021/09/20/cyber-attacks-russia-elections/
[32] Katherine E. et al. (2018). *Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies*. IFES. https://www.ifes.org/publications/cybersecurity-elections
[33] Council of Europe, CM-Rec (2017)5, 17 June 2017, Appendix I, sec. VIII. https://rm.coe.int/0900001680726f6f. This is a revision of the 2004 standards, which were the first of their kind.
[34] Council of Europe, CM-Rec. (2017)5, Appendix I, sec. VIII.
[35] United States Election Assistance Commission. (n.d.). *Voluntary Voting System Guidelines*. Voting Equipment. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

been captured in the Council of Europe's guidelines for certifying e-voting systems, which focused on selecting certification bodies, renewing certification, and conducting cost-benefit analyses.[36]

The field of cybersecurity in elections is still emerging, both in domestic law 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 cyber attacks.[37] 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.[38]

KEY SOURCES OF GUIDANCE FOR ADDRESSING ELECTION TECHNOLOGY AND CYBERSECURITY THREATS

- Council of Europe's 2017 e-voting standards
- Council of Europe's non-binding standards for e-voting
- Council of Europe's 2006 Cybercrime Convention (Budapest Convention)
- Various country-specific guidelines and laws

2. OPEN DATA, TRANSPARENCY, AND PRIVACY

International organizations and governing bodies have been actively establishing international principles pertaining to data and privacy for several decades. The United Nations (UN) General Assembly, for example, adopted its *Guidelines for the Regulation of Computerized Data Files* in 1990.[39] These guidelines require that data collectors be responsible for ensuring that data is accurate, transparently and lawfully collected, properly restricted to avoid discrimination, securely stored, and lawfully disseminated.[40] 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."[41] 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

[36] Secretariat, Council of Europe. (2011, February 16). *Certification of E-voting Systems: Guidelines for Developing Processes that Confirm Compliance with Prescribed Requirements and Standards*. GGIS (2010) 3 fin. E. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf8
[37] Council of Europe. (n.d.). *Budapest Convention on Cybercrime of the Council of Europe*. https://www.coe.int/web/cybercrime/the-budapest-convention
[38] 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. See: Solon, O. And A. Hern. (2017, June 28). *'Petya' Ransomware Attack: What is it and How Can it be Stopped?* Guardian. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
[39] United Nations General Assembly. (1990, December 14). *Guidelines for the Regulation of Computerized Data Files, 14 December 1990, res. 45/95*. http://www.refworld.org/pdfid/3ddcafaac.pdf
[40] Ibid.
[41] Ibid., sec. B.

or contamination by computer viruses."[42] 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.

The Open Government Declaration was signed by 75 countries in 2011, signaling their commitment to advancing transparency and openness within government.[43] It 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."[44] 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."[45] These standards are important for the adoption of voting and counting technology, in which individual information must be securely and transparently stored and checked to ensure the validity of both the voters and the votes.

Arguably the most prominent recent regulatory effort around data privacy is the 2018 passage of the European Union's (EU) General Data Protection Regulation (GDPR).[46] This regulation governs the collection, storage, and processing of EU residents by companies and organizations, and requires increased transparency about data storage and sharing.[47] Some analysts have noted that the GDPR "has been a catalyst for privacy regulation in other global jurisdictions,"[48] though approaches to data privacy taken in other regions may not mirror the EU approach.[49] At a global level, 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.

---

[42] Ibid., (7).
[43] Since joining in 2011, Hungary and Turkey withdrew their participation. Azerbaijan's status is inactive since 2015. See Open Government Partnership. *Open Government Declaration*. (n.d.). https://www.opengovpartnership.org/open-government-declaration.
[44] Ibid.
[45] Ibid.
[46] Regulation (EU) 2016/679. 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504
[47] European Commission. (n.d.). *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
[48] Marsh and McLennan Companies. (2020, August). *Two Years On, the GDPR Continues to Shape Global Data Privacy Regulation*. https://www.marsh.com/us/services/cyber-risk/insights/GDPR-two-years-on-continues-to-shape-global-privacy-regulation.html.
[49] Dipshan, Rhys. (2021, October 6). *GDPR's Global Impact May Be More Limited Than You Think*. https://www.law.com/legaltechnews/2021/10/06/gdprs-global-impact-may-be-more-limited-than-you-think-397-51646/?slreturn=20211023104029
[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.

KEY SOURCES FOR OPEN DATA, TRANSPARENCY AND PRIVACY PRINCIPLES

- Universal Declaration of Human Rights (UDHR)
- International Covenant on Civil and Political Rights (ICCPR)
- United Nations (UN) General Assembly Guidelines for the Regulation of Computerized Data Files
- European Parliament's General Data Protection Regulation (GDPR)
- United Nations Privacy and Data Protection Principles
- Open Government Declaration.

B. PRACTITIONER HANDBOOKS AND GUIDANCE DOCUMENTS

A 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 also contributed guidelines and handbooks on election technologies that are relevant to the discussion on cybersecurity.

The Commonwealth Secretariat publication "Cybersecurity for Elections: A Commonwealth Guide on Best Practice," included in the reading list annexed to this report, provides a high-level overview of cybersecurity good practices across the electoral process. This work also uses that standard framework to offer a more granular depiction of mitigating controls that can be implemented across the various technology processes commonly encountered during electoral preparation and administration.

In February 2018, the Center for Internet Security (CIS) published "A Handbook for Elections Infrastructure Security," which identifies election system threats and good practices that county or state election administrators in the United States could implement to mitigate those risks.[51] The Global Cyberalliance used this handbook to create the GCA Cybersecurity Toolkit for Elections, which provides free cybersecurity tools for election officials.[52] CIS also released a "Cybersecurity Supply Chain Risks in Election Technology" guide in 2021.[53]

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.[54] 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

[51] Calkin, B. Et al. (2018). *A Handbook for Elections Infrastructure Security*. Center for Internet Security. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[52] Global Cybersecurity Alliance. (2019). *The GCA Cybersecurity Toolkit for Elections*. https://gcatoolkit.org/elections/
[53] Garcia, M. and A. Wilson. (2021, February). *Managing Cybersecurity Supply Chain Risks in Election Technology A Guide for Election Technology Providers*. Center for Internet Security. https://learn.cisecurity.org/Managing-Cybersecurity-Supply-Chain-Risks-in-Election-Technology
[54] Mook, R., M. Rhoades and E. Rosenbach. (2018, February). *The State and Local Election Cyber-Security Playbook*. Harvard Kennedy School's Belfer Center, Defending Digital Democracy Project (D3). https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Election Officials" as well as an accompanying security planning checklist, which focuses on preventing and addressing technological failures, errors, and attack.[55] The Brennan Center's "A Framework for Election Vendor Oversight" notes that, in the U.S. context, "more than 80 percent of voting systems in use today are under the purview of three vendors. A successful cyber attack against any of these companies could have devastating consequences for elections in vast swaths of the country." Accordingly, they propose an oversight framework that includes an independent federal certification program; Congressional issuance of best practices for vendors in cybersecurity, among other areas; and ongoing review and enforcement of federal guidelines.[56]

In July 2018, the EU Cooperation Group[57] published a "Compendium on Cybersecurity 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]

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, which 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] publish and maintain comprehensive frameworks aimed at holistic management of cybersecurity risks through application of comprehensive controls and mitigations. In the absence of comprehensive election-specific cybersecurity standards, these general frameworks may be useful for EMBs. Accordingly, this section focuses on the general contours of these frameworks; their potential application in the electoral process is described in detail in later sections of this report.

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

---

[55] 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

[56] Norden, L., C. Deluzio and G. Ramachandran. (2019, November 12). *A Framework for Election Vendor Oversight: Safeguarding America's Election Systems*. Brennan Center for Justice at New York University School of Law. https://www.brennancenter.org/sites/default/files/2019-11/2019_10_ElectionVendors.pdf

[57] Comprising experts from the EU member states, the European Commission and the European Union Agency for Cybersecurity (ENISA).

[58] European Union Network and Information Security Cooperation Group. (2018, July). *Compendium on Cybersecurity of Election Technology*. https://www.ria.ee/public/Cyber_security_of_Election_Technology.pdf

[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] The National Institute of Standards and Technology's website is found at: https://www.nist.gov/.

[61] The ISACA website can be found at: https://www.isaca.org/.

[62] The International Organization for Standardization's website can be found at: https://www.iso.org/home.html.

[63] The U.S. Computer Emergency Readiness Team's (US-CERT) website can be found at https://www.us-cert.gov/.

framework in five steps that is now widely used within the cybersecurity community: identify; protect; detect; respond; and recover. NIST 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]

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 Kremlin involvement in the 2016 U.S. elections, ransomware, and insider threats.[68] The diverse landscape of threats from inside and outside an organization demonstrates 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 (including technology and physical sites like polling places) 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]

---

[64] Shemlse Gebremedhin Kassa. (2016). *Information Systems Security Audit: An Ontological Framework*. ISACA Journal vol. 5. https://www.isaca.org/Journal/archives/2016/volume-5/Pages/information-systems-security-audit.aspx.
[65] ISACA. (n.d.). *COBIT: An ISACA Framework*. https://www.isaca.org/resources/cobit
[66] ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Publisher: ISACA.
[67] International Organization for Standardization and International Electrotechnical Commission. (2011). *ISO/IEC 27005:2011*. https://www.iso.org/standard/56742.html; and European Union Agency for Network and Information Security. (2018, January 15). *ENISA Threat Landscape Report 2017*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[68] European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2017*, pp. 79-87.
[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

D. ACADEMIC LITERATURE

The academic literature on election cybersecurity offers an array of perspectives and analysis on the points throughout the election process that may be vulnerable to cyber attacks, and strategic recommendations to mitigate risk. While relevant academic research has been cited throughout this paper, this section focuses on a brief summary of the literature divided into two relevant sections: academic research on key vulnerabilities across the electoral process; and a deeper dive into voting technologies, the subject of significant scholarly analysis.

1. VULNERABILITIES ACROSS THE ELECTORAL PROCESS

Researchers have identified vulnerabilities across various stages of the election process. One of the earliest vulnerabilities, as identified by Shackelford et al., is the opportunity for cyber attackers to target critical information used by voters in the lead up to elections;[71] within this stage, researchers note cyber attackers could target political parties and candidates[72]or attempt to alter information regarding voting requirements or voting locations listed on official websites.[73] A subsequent point of risk would be an attack on voter registration systems as well as voter rolls used during elections to verify the identities of voters. At this point, researchers note cyber attackers could deter voters by rendering voter registration websites unavailable via DDOS attacks,[74] compromise the integrity of registration databases by adding fake voter records, or steal voter data from the database.[75] The remaining three points of risk include targeting voting machines and mechanisms to cast votes; the mechanisms used to tabulate votes; and the process by which the results of an election are disseminated.[76]

Key Findings on Cyber Attacks and Elections from Academic Literature

Highly vulnerable targets include:

- Informational websites (e.g., on voting requirements and polling locations)
- Voter rolls
- Voting machines and mechanisms*
- Vote tabulation equipment*
- Results announcement processes
- Candidate and party databases

*Physical equipment or machinery is vulnerable at many stages along the supply chain from design to disposal

Academic recommendations for preventing and addressing cyberattacks include:

- Designate elections-related infrastructure, including technology, as critical (enabling increased government assistance to protect software, equipment, people and processes)
- Updating legal frameworks and standards to address emerging vulnerabilities
- Domestic centralization of data
- International and domestic information sharing and identification of good practices
- Certification of vendors that meet cybersecurity guidelines
- Raising voter awareness around types of cyberattacks and mis- and dis-information campaigns in elections

[71] Shackelford, S. et al. (2017). *Making Democracy Harder to Hack*, 50 U. Mich. J. L. Reform 629. https://repository.law.umich.edu/mjlr/vol50/iss3/3
[72] Shackelford et al., *Making Democracy Harder to Hack.*
[73] Dawood, Y. (2021). *Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats*. Election Law Journal: Rules, Politics, and Policy, 20(1), 10-31. http://doi.org/10.1089/elj.2020.0652
[74] Garnett, H. & James, T. (2020). *Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity*. Election Law Journal: Rules, Politics, and Policy, 19(2), 111-126. http://doi.org/10.1089/elj.2020.0633
[75] Dawood, *Combatting Foreign Election Interference.*
[76] Shackelford et al., *Making Democracy Harder to Hack.*

As noted, cyber attackers may also go beyond targeting official election sources, data, and equipment to influence election outcomes. Tenove et al., highlight the possibility for cyber attackers to gain access to candidate and party data and subsequently release damaging information to influence results. They note this may impact election integrity beyond a singular election by possibly dissuading candidates from participating in the future.[77] Supply chains are another possible point of risk. Within the supply chain, researchers outline various access points where cyber attackers may be able to target election equipment beginning with the design phase and proceeding with the manufacturing of the equipment and equipment parts, the equipment assembly, the equipment warehousing, distribution, and lastly once equipment is no longer re-sold or disposed of, during when malign actors could gain access to equipment widely used in a country's elections.[78]

The scholarly literature also outlines a range of recommendations to bolster election cybersecurity as well as to deter future cyber attacks. One key policy recommendation suggested by researchers includes designating election technology, equipment and processes as critical infrastructure, which can open up election systems to receive additional government assistance,[79] though others note that such a designation may result in political opposition as well as new foreign policy implications.[80] Additional policy recommendations include reviewing electoral laws, updating international standards,[81] developing countermeasures that address foreign state interference and attacks,[82] centralizing the collection of foreign interference data,[83] and furthering information sharing via international forums with other democratic countries[84] and with trusted expert groups.[85] A final set of recommendations focus on the efficacy of expanding communications on security efforts to build voter trust.[86] Research analyzing the experiences of election officials in Texas highlights, for example, that improvements to election security are only one part of a broader solution to build trust; in the Texas example, the spread of misinformation campaigns undermined voter trust in the election process.[87] Working to combat misinformation and communicate evidence of security to voters, the researchers note, will be critical to ensuring election integrity moving forward.[88] Communication with political leaders to inform them of existing risks is another possible area to strengthen cybersecurity awareness.[89]

---

[77] Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy. Research Report, Centre for the Study of Democratic Institutions, University of British Columbia. http://dx.doi.org/10.2139/ssrn.3235819

[78] Hodgson, Q. E., Brauner, M. K., Chan, E. W. (2020). *Securing U.S. Elections Against Cyber Threats: Considerations for Supply Chain Risk Management*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PEA512-1.html

[79] Fidler, D. P. (2017). *Transforming Election Cybersecurity*. Council on Foreign Relations. https://www.cfr.org/report/transforming-election-cybersecurity.

[80] Shackelford et al. "Making Democracy Harder to Hack."

[81] Garnett and James, *Cyber Elections in the Digital Age.*

[82] Fidler, *Transforming Election Cybersecurity.*

[83] Henschke, A., Sussex, M., & O'Connor, C. (2020). *Countering Foreign Interference: Election Integrity Lessons for Liberal Democracies*. Journal of Cyber Policy, 5(2), 180-198. DOI: 10.1080/23738871.2020.1797136

[84] Fidler, *Transforming Election Cybersecurity.*

[85] Henschke, Sussex, and O'Connor, *Countering Foreign Interference.*

[86] Fidler, *Transforming Election Cybersecurity.*

[87] Kasongo, E., Bernhard, M., & Bronk, C. (2021). *Tales from the Trenches: Case Studies in Election Cybersecurity Preparedness in Texas*. E-Vote-ID 2021, 113.

[88] Ibid.

[89] Henschke, Sussex, and O'Connor, *Countering Foreign Interference.*

2. VOTING TECHNOLOGY

Though the scholarly literature on cybersecurity and elections covers a wide breadth of topics, research on various forms of electronic voting (including in-person electronic voting via direct-recording electronic voting machines [DREs]; remote, paperless voting, including internet voting; and certain applications of blockchain-based voting[90]) comprise a critical component of this scholarship. Given this emphasis, this subsection will provide a more targeted view of key academic literature in this area.

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).[91] 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.

In the United States, Feldman et al., identify critical vulnerabilities of the Diebold AccuVote-TS machine, a DRE machine that was widely used in the 2006 United States general election.[92] Feldman et al., demonstrate that 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.[93] Tests conducted by researchers on DRE machine systems in California and Ohio yielded similar results.[94] In India, a test of one 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.[95] 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.[96] The results of this

[90] Blockchain is a technology that utilizes a decentralized method to record and track transactions. A digital ledger of transactions is duplicated across many computers and each duplicated ledger is updated as transactions occur. Each transaction carries a digital signature and timestamp to ensure the validity. Since the technology was developed to overcome issues of trust and with tamper resistance in mind, the technology may be useful in electoral contexts. Further information about the general technology can be found at the NIST Blockchain Overview available at: https://www.nist.gov/blockchain.

[91] Gambhir, R. K., & Karsten, J. (2019). *Why Paper Is Considered State-of-the-Art Voting Technology*. Brookings Cybersecurity and Election Interference. https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/; and 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. https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today; and 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

[92] Feldman, Halderman, and Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*.

[93] Ibid.

[94] Balzarotti, D., et al. (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.

[95] Wolchok, S., et al. (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).

[96] 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).

review contributed to the retirement of the NEDAP ES3B in the Netherlands and a return to paper voting.[97]

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.[98] DREs lack a paper trail; pairing a DRE machine with another system that creates a paper record of a vote can support the auditability of DRE machines and help officials identify attacks.[99] An election that is both auditable and audited satisfies the conditions to be considered an evidence-based election.[100] 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.[101]

There is broad consensus on the cybersecurity risks of DRE machines lacking a voter-verifiable paper audit trail.[102] Still, election officials globally have begun to embrace, pilot, and implement internet voting technology,[103] even though analyses 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.[104] Similarly, experimental attacks of a reproduction of Estonia's voting system,[105] the first in the world that used internet voting at the national level, and of a Washington D.C. online voting pilot tool[106] 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.[107] Moreover, researchers cite the possibility of blockchain technology to replace paper-based election

---

[97] National Democratic Institute. (n.d.). *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

[98] MIT Election Data + Science Lab. (n.d.). *Voting Technology*. https://electionlab.mit.edu/research/voting-technology

[99] Mook, Rhoades, and Rosenbach, *The State and Local Election Cyber-Security Playbook*; and Norden, Cordova McCadney, *Voting Machines at Risk.*

[100] 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

[101] Feldman, Halderman, and Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine,* p. 14.

[102] Gambhir and Karsten, *Why Paper Is Considered State-of-the-Art Voting Technology.*

[103] Park, Specter, Narula, and Rivest, *Going from Bad to Worse.*

[104] 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

[105] Springall, D., et al. (2014). *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.

[106] 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

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

systems and outline the cost-savings and beneficial impacts to transparency and participation it could provide.[108]

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,[109] 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.[110] 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."[111] A description of Voatz' security model is not publicly available, but the app's owner claims blockchain is one of multiple components used to safeguard the application.[112] 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.[113] Further exploration may be required to understand the capability of this technology to adequately safeguard remote voting systems.

III. APPLYING A RISK-BASED LENS TO 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.

A. RISK MANAGEMENT FRAMEWORKS

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;[114] the International Organization for Standardization (ISO) 31000 series, which is a generic risk management framework and

[108] Ibid.
[109] Park, Specter, Narula, and Rivest, *Going from Bad to Worse*.
[110] Ibid.
[111] 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).
[112] Ibid.
[113] Gaudry, P., and A. Golovnev. (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.
[114] NIST SP 800-37 is specific to the information technology concepts. It is available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

can be applied in conjunction with ISO 27001 IT controls.[115] 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.[116] 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.

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. [117]

Risk Management as a Continuous 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.

B. CONTROLS, TRANSFERRANCE AND ACCEPTANCE

While the premise is simple, operationalizing cybersecurity risk management in electoral cycles is not a trivial task. Security controls are descriptions of discrete actions that can be taken to help mitigate risks.[118]

[115] The ISO 31000 framework is a general risk management framework that can be applied in various contexts, not just IT. 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.
[116] European Union Agency for Cybersecurity. (n.d.). *ENISA RM/RA Framework*. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework
[117] This is a simplification for understanding and brevity of the process described in depth within NIST, ISO, ENISA and other risk management frameworks.
[118] NIST SP 800-53 Rev. 5 defines a core set of security and privacy controls that operationalize the framework elucidated in 800-37. U.S. Department of Commerce and National Institute of Standards and Technology. (2020, September). *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Different frameworks separate controls into various aggregations, but the following three categories are useful for this discussion:[119] management controls, operational controls, and technical controls.

COMMON CATEGORIES OF SECURITY CONTROLS		
MANAGEMENT CONTROLS	OPERATIONAL CONTROLS	TECHNICAL CONTROLS
Management controls are safeguards that focus on identifying and mitigating risks to information security through the use of assessments, audits, and planning.[120]	Operational controls are safety and security measures that are implemented and executed by human beings as they use, interact, and manage electronic information systems. [121]	Technical controls are safeguards that are generally embedded within hardware, software and firmware to protect information. A common example is encryption.[122]

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).

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 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,

[119] 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. See: Center for Internet Security. (n.d.). The 18 CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list/

[120] Ibid., p. 9.

from procurement through disposal, within the defined risk management framework.[121] Controls also involve defining the mechanisms of response during cybersecurity incidents.[122] 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).[123]

C. ADOPTING AND ADAPTING RISK MANAGMENT STRATEGIES

Effective cybersecurity requires buy-in at the executive level, 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. It is therefore unsurprising to note that EMBs have, generally, been slow to adopt comprehensive cybersecurity risk management programs using dedicated resources and professional roles.

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."[124] In other cases, EMB executives may have unrealistic expectations that new technologies will have a positive impact on electoral processes. Successfully introducing, managing and cost-effectively maintaining technologies can be highly complex and challenging. This is especially the case in countries where the election authorities have

"One fundamental problem is that the discussion, decision and implementation of new technology sucks out too much oxygen of many EMBs who have limited time and resources. Not only do many 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."

- Peter Erben, "Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches," p. 3, 2017.

[121] 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.
[122] The particulars of which are also not defined nor developed within the present discussion.
[123] 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.
[124] Erben, Peter. (2017). *Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches*. International Foundation for Electoral Systems. https://www.ifes.org/sites/default/files/ifes_erben_raising_trust_in_electoral_technology_innovation_aided_by_traditional_approaches_d8_sep_2017.pdf

limited previous experiences in holistically reviewing the risks and rewards of the investment. Too often, technology has been introduced to overcome what is inherently a political issue, lack of proper planning within the EMB, or to overcome the Commission's insufficient quality control capabilities of its field operations.

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.

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.

The concept of *maturity* is widely used in the cybersecurity community to refer to the ability and capacity of a cybersecurity program to help an organization to identify, detect, deter, and respond to threats unique to their organization or field. Maturity models help organizations locate their baseline cybersecurity activity on a scale and identify their desired future state. 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

Illustrative Maturity Model [127]

Level 3: Adaptable and proactive cybersecurity posture

Level 2: Cybersecurity practices are documented and there is institutionalized support and resources for those documented processes. The organization may still take a reactive approach to cybersecurity.

Level 1: Some practices and capabilities are in place, albeit ad hoc in nature

Level 0: Absence of cybersecurity activities and practices

[125] 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 here: Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy. (n.d.). *Cybersecurity Capability Maturity Model (C2M2)*. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

maturity to determine the baseline skillset required of persons filling those roles.[126]

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.[127]

The following sub-section will present a short discussion of cyber adversaries. It is followed by content on illustrative threats, vulnerabilities, and mitigation across various components of 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.

D. THREAT ACTORS

A key part of assessing cybersecurity risk means understanding, as fully as possible, the threat actors. This discussion will define categories of actors and speak briefly about the types of tactics, techniques, and procedures employed by such adversaries. Tactics, Techniques, and Procedures (TTPs), as a concept, are broadly used by the 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.[128]

Disinformation as a tactic to undermine public confidence has emerged as a key component within the election 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

[126] Available here: National Initiative for Cybersecurity Careers and Studies. (n.d.). *Workforce Framework for Cybersecurity (NICE Framework)*. https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[127] One such example of the integrating ISO 27001 standards can be found in the Republic of Moldova: Republic of Moldova (2017). *Central Electoral Commission: 20 Years of Permanent Activity*. https://a.cec.md/storage/old_site_files/files/files/20%20ani%20CEC/Cartea_Cec_20_ani_eng_compressed.pdf
[128] For a comprehensive discussion of TTPs that maps selected tactics, techniques, and procedures to specific tools and methods for specific threat actors, see the MITRE ATT&CK framework available here: MITRE. (n.d.). Att&ck. https://attack.mitre.org

demagoguery has led to multi-million-dollar tort suits by the election technology industry.[129] Worse, it has eroded public confidence in elections among large segments of the electorate.[130] 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.

The categories below are introduced to support basic understanding of the different types of actors that may pose a threat to elections, but they do not operate in silos. Foreign state actors may cooperate with domestic political groups or criminal groups for example, where their objectives align.

1. FOREIGN STATE ACTORS AND ADVANCED PERSISTENT THREATS

Malicious actors associated with or directly tied to foreign governments constitute a grave threat within the election security space. Assessing the objectives and motivations of such actors can be difficult; however, there is general consensus among analysts that many malicious foreign actors are seeking to undermine democratic institutions and sow political discord.[131] Specific motivations and objectives may vary from target to target and among the purveyors of such attacks. The Kremlin's motivations, for example, are assessed by some analysts to be focused on generally undermining democratic institutions while the People's Republic of China may be using a more targeted approach to influence specific foreign policy goals and interests.[132] Malicious threat actors associated with foreign governments are generally 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.[133] APT 29, also known within the industry as "Cozy Bear," is attached to the Russian Foreign Intelligence Service (SVR).[134] Both groups have been responsible for some of the highest visibility and

[129] Dean, G. & Shamsian, J. (2021, August 14). *From Mike Lindell to OAN, Here's Everyone Dominion and Smartmatic are Suing over Election Conspiracy Theories So Far.* Business Insider. https://www.businessinsider.com/everyone-dominion-smartmatic-suing-defamation-election-conspiracy-theories-2021-2?op=1

[130] Laughlin, N., and P. Shelburne. (2021, January 27). *How Voters' Trust in Elections Shifted in Response to Biden's Victory.* Morning Consult. https://morningconsult.com/form/tracking-voter-trust-in-elections/

[131] For the American context see recent U.S. Director of National Intelligence report: National Intelligence Council. (2021, March 10). *Foreign Threats to the 2020 U.S. Federal Elections.* https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

[132] Hanson, F., S. O'Connor, M. Walker, and L. Courtois. (2019). *Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections*. International Cyber Policy Centre. https://apo.org.au/node/236546

[133] Mitre Att&ck. (n.d.). *APT28*. https://attack.mitre.org/groups/G0007/; and Crowdstrike. (2021, April 1). *What is an Advanced Persistent Threat (APT)?* https://attack.mitre.org/groups/G0007/ and https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[134] Mitre Att&ck. (n.d.). *APT29*. https://attack.mitre.org/groups/G0016/

effective cyber operations against elections entities over the past several years.[135] 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 therefore cannot be easily defended against. APT 28 and APT 29 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.[136]

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 (in the election arena, this may include, for example, EMB commissioners and key IT personnel, current incumbents or candidates for high-level office and the leadership of major political parties). 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. The People's Republic of China, Iran, and North Korea all have sophisticated offensive cyber operations that leverage APT level tools, tactics, techniques, and procedures.[137]

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.[138] 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.[139] These actors can work independently, but also sometimes coordinate with clandestine services, criminal or independent groups to achieve their aims. Government actors can also make use of their own means of surveillance to pressure, intimidate, expose damaging private information, or prosecute electoral stakeholders seen as problematic or contrary to the interests of political actors in control of state resources. Examples of such tactics include the way Saudi Arabia utilized mobile phone spyware purchased from an Israeli company to monitor dissidents and political opponents.[140]

---

[135] Burgess, M. (2017, November 1). *Exposed: How One of Russia's Most Sophisticated Hacking Groups Operates.* Wired Magazine. https://www.wired.co.uk/article/how-russian-hackers-work

[136] Ibid.

[137] Mandiant. (n.d.). *Advanced Persistent Threat Groups.* https://www.mandiant.com/resources/apt-groups

[138] See Lindberg, S. (ed.). (2021, March). Autocratization Turns Viral: Democracy Report 2021. https://www.v-dem.net/files/25/DR%202021.pdf

[139] Robertson, J., M. Riley, and A. Willis. (2016, March 31). *How to Hack an Election: Andres Sepulveda Rigged Elections throughout Latin America for Almost a Decade. He Tells His Story for the First Time.* Bloomberg. https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[140] Bergman, R. and M. Mazzetti. (2021, November 3). *Israeli Companies Aided Saudi Spying Despite Khashoggi Killing.* New York Times. https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

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.[141] Sometimes, however, it is suspected that criminal groups will work in concert with governments or foreign threat actors for either financial remuneration, 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.[142]

4. NON-STATE POLITICAL GROUPS AND HACKTIVISTS

Criminal activity attributed to non-state political groups (including political parties and candidates themselves engaging in malicious activity) and activist individuals can also potentially target election-related infrastructure and other parties, candidates, or related (e.g., fundraising, and political) organizations. Hacktivist is a term used to describe the blending of hacking and activism regarding political and social issues. While there are no specific examples of attacks by hacktivists or non-state political groups against election infrastructure at the time of this writing, there are many examples of hacktivist attacks against other governmental IT infrastructure in several countries and within the United States.[143] This activity can be organized and domestically-based, and can be driven by transnational collaborators or individuals.[144] In addition, there are examples of foreign governments hiring hackers outside of their borders to carry out attacks on their behalf, blending the category of foreign state actors and non-state groups.[145]

5. 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 –

---

[141] Fung B. (2020, October 29). *Ransomware Hits Election Infrastructure in Georgia County.* CNN. https://edition.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html; and Organization for Security and Co-operation in Europe. (2019, August 21). *Republic of North Macedonia, Presidential Election, 21 April and 5 May 2019, ODIHR Election Observation Mission Final Report.* https://www.osce.org/files/f/documents/1/7/428369_1.pdf

[142] Vrabie, V. et al. (n.d.). *More Evidence of APT Hackers-for-Hire Used for Industrial Espionage*. Bitdefender. https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[143] Bergal, Jenni. *'Hacktivists' Increasingly Target Local and State Government Computers.* PEW. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/01/10/hacktivists-increasingly-target-local-and-state-government-computers

[144] George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), 100249.

[145] Department of Justice Office of the United States Attorneys. (2018, May 29). *International Hacker-For-Hire Who Conspired With And Aided Russian FSB Officers Sentenced To Five Years In Prison*. https://www.justice.gov/usao-ndca/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-five

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 an insider threat. In terms of technical controls, automated alerting of suspicious activity such as copious printing 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. EMB RISK MITIGATION ACROSS THE ELECTORAL PROCESS

Election processes are complex and multifaceted, and vary across democratic systems and contexts. The following subsections highlight the technologies and processes involved with various important tasks in elections, with an emphasis on cybersecurity risks, threats, and mitigation strategies. The controls discussed throughout this sub-section are considered 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.

SELECT STRATEGIES FOR EMBS TO MITIGATE AND ADDRESS CYBER THREATS IN ELECTIONS

All functional teams in an EMB can and should contribute to a continuous and holistic culture of cybersecurity both within the institution and among voters: legal, communications, media/public affairs, operations, procurement, as well as information technology.

An EMB's government, peer organizations, and vendors are critical partners in reinforcing a local and international culture of cybersecurity.

Read further for more information but in general, EMBs should:

- Use the concept of least privilege to maintain control of sensitive information and systems, and use clear criteria for when access is allowed and when it should be revoked.
- Enable encryption, test and standardize security settings, and harden/limit functionality of hardware and software, especially remote/internet access.
- Design full chains of custody with regular integrity checks for all electronic and physical assets, from initial procurement to the end of life and disposal for the asset as required by law and in accordance with good practice.
- Practice, test, and simulate a variety of cybersecurity events and attacks, ideally with partners or independent parties. This produces valuable data for an EMB's procurement, security, response, and recovery plans—which, to emphasize, should involve all functional teams.
- Recognize the benefit of improved cyber hygiene and regular training at every level (high-profile political targets, candidates; judges, lawyers, clerks; election staff to EMB leadership and voters/general public).
- Maintain transparent, accessible systems with paper backups for results, audits, decisions, complaints and their responses. Paper backups are also useful tools in certain, but not all operational contingency plans.

A. LEGAL AND REGULATORY CONTEXT

1. CONSIDERATIONS FOR INTRODUCING NEW ELECTION TECHNOLOGY

The specific **operational context** for elections must be carefully considered before introducing, procuring, and 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.[146] New technology typically requires additional human capital considerations, such as stronger information technology (IT) skills and experience as many election staff lack the skills to manage new technology without training.[147] In Kosovo in 2010, for example, 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.[148] This example 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.

In addition to the operational context, the **structure of the electoral legal framework** may also 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)."[149] In some cases, legislation governing these technologies may be found in areas outside of elections, such as regulations on data protection.[150] 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."[151] 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."[152]

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. 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

---

[146] Yard, M. (ed.). (2011). *Civil and Voter Registries: Lessons Learned from Global Experience.* International Foundation for Electoral Systems. p. 8; and; European Commission. (2006). *EC Methodological Guide on Electoral Assistance*. https://www.eods.eu/library/EC%20Methodogical%20Guide%20on%20Electoral%20Assistance%202006.pdf. pp. 59-60.
[147] Yard (ed.), *Civil and Voter Registries*, p. 157.
[148] Ibid., 42.
[149] Goldsmith, B. and H. Ruthrauff. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. National Democratic Institute and International Foundation for Electoral Systems. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies. p. 106.
[150] Organization for Security and Co-operation in Europe. (2013, October 1). Guidelines for Reviewing a Legal Framework for Elections, Second Edition. https://www.osce.org/odihr/elections/104573, pp. 65-69.
[151] Yard, M. (ed.). (2010, September). Direct Democracy: Progress and Pitfalls of Election Technology. International Foundation for Electoral Systems. p. 21.
[152] Council of Europe. (2011, February 16). *Guidelines on Transparency of E-Enabled Elections.* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf6

trust in the process.[153] A fundamental element 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.

Legal framework and timeframe challenges may compound each other. For instance, 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, tight procurement timelines to meet legally mandated election dates might result in insufficient time for effective testing and training (or lead to criticism of the EMB for undertaking emergency or sole source procurements). Provisions in the law may also impact timelines for adoption of new technologies. 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.

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.[154] If public trust in the electoral process is already low, introduction of a new system may cause public unrest.[155] 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."[156] In addition to the voting public, political parties should be consulted. Explicit buy-in from all involved political parties regarding technology and technology implementation can mitigate against contestation later in the electoral process - avoiding costly litigation, audits, and recounts.

Specific tools that provide independent ways to test the system, such as audits of technology systems, are also a good means to gain public trust and secure against fraud.[157] 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. As highlighted earlier in the academic literature review, an analysis of Texas counties during the 2020 United States elections conducted by Kasongo et al., highlights that improvements to training, resources, and processes, while helpful for ensuring a smoother election process, may not be sufficient to mitigate

[153] European Commission and United Nations Development Programme. (2010). *Procurement Aspects of Introducing ICT Solution in Electoral Processes.* https://www.undp.org/publications/procurement-aspects-introducing-ict-solutions-electoral-processes. p. 55.
[154] European Commission. (2006). *EC Methodological Guide on Electoral Assistance.* https://www.eods.eu/library/EC%20Methodogical%20Guide%20on%20Electoral%20Assistance%202006.pdf. p. 57.
[155] Council of Europe. (2017, June 14). *Guidelines on the Implementation of the Provisions of Recommendation CM/Rec (2017) 5 on Standards for E-Voting*. CM-Rec(2017)50.
[156] Catt, H., et al. *Electoral Management Design, revised ed*. International IDEA. pp. 266-267.
[157] European Commission, *EC Methodological Guide on Electoral Assistance*, p. 63.

the spread of disinformation and preserve voter trust. The researchers note that proactively using evidence to demonstrate to voters that elections were conducted securely will be key to building voter confidence and addressing misinformation, especially when standard challenges during an election emerge.[158] As technology is introduced, robust information campaigns should be implemented to make sure the technologies are well understood by the voting public and other stakeholders. The costs of such educational programs must be planned and understood as part of a holistic procurement strategy. In addition, as technology is utilized and situations arise that call into question the reliability or security of that technology, election officials are best served by transparently communicating such issues and their resolution in order to maintain and bolster public confidence.

Other mechanisms can 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.[159] 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.[160] 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.[161]

2. CYBERSECURITY-SPECIFIC LEGAL AND REGULATORY FRAMEWORK CONSIDERATIONS

When drafting the legal and regulatory framework surrounding elections, the following questions related to cybersecurity, at a minimum, should be clearly answered within the election law and relevant regulations:

1) Who is responsible and liable for ensuring the cybersecurity of newly procured technology (the vendor or state agency procuring the technology)?
2) Which state actor is responsible for auditing, testing, and certifying election technology before its deployment?
3) Does the law require transparency of the testing, auditing and certification process?
4) Does the law define the duty of care of the institutions that have access privileges and that use election technology?

---

[158] Kasongo, E., Bernhard, M., & Bronk, C. (2021). Tales from the Trenches: Case Studies in Election Cybersecurity Preparedness in Texas. E-Vote-ID 2021, 113.
[159] Shein, E. and A. Brown. (2021). *Risk-Limiting Audits: A Guide for Global Use.* The International Foundation for Electoral Systems. https://www.ifes.org/sites/default/files/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf
[160] Ibid.
[161] Ibid.

5) Does the law clearly define data privacy protection requirements of stakeholder and election electronic election data vis-à-vis data recorded on paper (especially results data); and put in place protections (e.g., a paper trail) and clear steps that should be taken if a cybersecurity breach impacts election result data or data transmission?
6) As part of trust building process, does the law allow for and provide guidance and resources for EMBs and EDR tribunals to ascertain that election technology was secure throughout an election (i.e., to prove to stakeholders that electoral systems were not penetrated by cyber attacks and therefore that voter registers, voting and results remained unaffected)?
7) If a cyber attack is detected, what actions or processes would the law trigger (e.g., an audit, full recount, annulment or rerun);[162] which institution would oversee these processes (the EMB or the EDR court, or the national cybersecurity agency); would the private sector or third parties be allowed to conduct testing and audits (as is the case in Iraq);[163] whether election technology equipment would be considered to be compromised once it is accessed by a third party (as in Arizona in 2021)?[164]
8) Does the law indicate the cybersecurity standards that must be met when procuring election technology, ownership and access permissions for the source code; and the procedures for replacing a compromised EVM?
9) What are the remedies, as defined in the law, available for individuals when their data privacy rights have been breached or for candidates and other stakeholders when other election related data has been compromised?

If the law and regulatory framework clearly answers these questions, it will provide EMBs and other electoral institutions both notice of and guidance for how they can meet the challenge of adapting to existing cybersecurity risks. 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 also dictate that sufficient time be allocated to adapt the legal and regulatory framework prior to 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 notes 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-

[162] See for example: de Freytas-Tamura, K. (2017, September 1). *Kenya Supreme Court Nullifies Presidential Election*. New York Times. https://www.nytimes.com/2017/09/01/world/africa/kenya-election-kenyatta-odinga.html
[163] UN Assistance Mission for Iraq. (2021, September 9*). Iraq's Electoral Preparations and Processes Report No. 11*. https://reliefweb.int/report/iraq/iraq-s-electoral-preparations-and-processes-report-no-11-9-september-2021. Also see the following source for an example from a different country context: teleSUR. (2021, February 21). *Ecuador's Comptroller to Audit Electoral Computer System*. https://www.telesurenglish.net/news/Ecuadors-Comptroller-to-Audit-Electoral-Computer-System-20210221-0003.html
[164] Timm, J. (2021, May 20). *Maricopa County will Need New Voting Machines after GOP's Audit, Arizona Secretary of State Says.* NBC News. https://www.nbcnews.com/politics/elections/maricopa-county-will-need-new-voting-machines-after-gop-s-n1268090

voting. The role and the responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level."[165]

CYBERSECURITY IN THE PHILIPPINES ELECTION PROCESS

In March 2016, the website of the Philippines Commission on Elections (COMELEC) was hacked by a group called Anonymous Philippines. The hacker group LulzSec Pilipinas also released extensive voter information, including fingerprints. Following the attack, the National Privacy Commission recommended criminal charges against COMELEC Chairperson Andres Bautista for negligence, stating that "The lack of a clear data governance policy, particularly in collecting and further processing of personal data, unnecessarily exposed personal and sensitive information of millions of Filipinos to unlawful access."[166]

While the Commission did not find Bautista guilty of helping with the attack, it 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, after a computer containing biometric records of registered voters was stolen from a regional election office,[167] Chairperson Bautista was impeached and resigned. 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 the role that privacy commissions may play in oversight of personal data in elections.

B. PROCUREMENT AND PLANNING

Overview and main uses of technology: Planning and procurement for election operations begins well before Election Day, and cybersecurity must be addressed for each component, including procuring information and communication technology (ICT) systems, websites, social media and communication platforms; and managing physical locations, personnel, training and budgeting. Often electronic information systems are thought of within the context of a "life-cycle" that begins at procurement stage and lasts through retirement and disposal of the system. Cybersecurity planning is needed throughout the life-cycle of each system used by the election administration.

Proper security planning and field-testing with the relevant cybersecurity, law enforcement, military, and private security stakeholders is also important throughout all phases of the electoral process. 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.[168]

Despite these imperatives, procurement processes are often truncated, because of time constraints or EMB relations with favored vendors that undermine effective bid evaluation of cybersecurity criteria. Cybersecurity is also often given insufficient attention when drafting technical specifications for tenders,

[165] See Standard 29 in: Ad Hoc Committee of Experts on Legal, Operational and Technical Standards for E-Voting, Council of Europe. (2017, June 14). *Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on Standards for E-Voting*. https://rm.coe.int/168071bc84

[166] National Privacy Commission. (2017, January 5). *Privacy Commission Recommends Criminal Prosecution of Bautista over Comeleak.* https://www.privacy.gov.ph/2017/01/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/

[167] National Privacy Commission. (2017, February 20). *NPC Starts Probe into COMELEC's 2nd Large Scale Data Breach; Issues Compliance Order.* https://www.privacy.gov.ph/2017/02/npc-starts-probe-comelecs-2nd-large-scale-data-breach-issues-compliance-order/

[168] National Conference on State Legislatures. (2021, November 5). *Voting Systems Standards, Testing and Certification.* https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

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 the acquisition of EVMs on grounds that machines could compromise secrecy of the ballot and would need to be introduced gradually to ensure they were secure from tampering and would not enable fraud.[169] Many countries also do not allow independent observation of election technology testing, which detracts from stakeholder confidence in that technology's protection against cyber attack.[170]

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. 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.

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 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.[171]
- 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.[172]
- 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 controls to

[169] The Express Tribune. (2021, September 10). *Key Clauses of Electoral Reforms Bill Rejected.* https://tribune.com.pk/story/2319515/senate-body-rejects-use-of-evms-in-next-elections; and The News. (2021, September 8). Election Commission Rejects EVM.
[170] Golos Info. (2020, July 29). Statement on the New Remote Electronic Voting System of the CEC of Russia. https://www.golosinfo.org/articles/144545
[171] Abawajy, J. (2014). *User Preference of Cybersecurity Awareness Delivery Methods*. Behavior & Information Technology, 33(3), 237-248.
[172] Shinde, N., & Kulkarni, P. (2021). *Cyber Incident Response and Planning: a Flexible Approach*. Computer Fraud & Security, 2021(1), 14-19.

maintain control of data as it traverses organizational boundaries, and to prevent proprietary data from leaving designated infrastructure.[173]

- 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.

UNDERTAKING PROACTIVE COMMUNICATIONS IN PARALLEL WITH PROCUREMENT

EMBs should not introduce new technology without an extensive communication and awareness campaign to inform stakeholders. **Procurement and operationalization of new technology should automatically trigger consideration of 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.

C. 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.[174] Technology has been increasingly integrated into these processes, replacing mostly cumbersome manual systems that precisely map locations and distribute voters. Technology, when part of a transparent and impartial process, can contribute to processes that distribute voters equitably, that maintain standards of vote weight and ensures the representativeness and non-discrimination nature of electoral districts. [175] This same technology, when used to manipulate electoral districts and boundaries, can be a very effective tool in efforts to gerrymander election districts and manipulate electoral outcomes.

Risk discussion: There have not been any reported attacks against the electoral process using boundary delimitation tools or access. EMBs should consider, however, that 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). 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.

[173] Liu, S., & Kuhn, R. (2010). *Data loss prevention*. IT professional, 12(2), 10-13.
[174] Handley, L. (2007). "Boundary Delimitation." In *Challenging the Norms and Standards of Election Administration*, International Foundation for Electoral Systems. 59-74.
[175] Ibid.

Mitigation strategies:

- **When systems are connected 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**. In some contexts where the agencies providing data cannot guarantee their integrity, physical transfer (via a USB device) to an air-gapped[176] rather than electronic transfer to a connected database can be advisable.
- **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.**

D. 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' personally identifiable information (PII). The degree of automation, the type of data, and the range of services varies depending on a country's legal framework and the election administration's eagerness to deploy new technologies.

Over the past decade, the use of biometric voter registration (BVR) has risen steadily. In Africa in particular, more than 25% of countries now use biometric data during the electoral process. BVR is a mature technology, most often based on facial features and fingerprints, that collects and analyzes voters' unique characteristics. It is considered to be an effective mechanism to prevent multiple registration, and to verify identity and eligibility to vote. BVR has significant limitations, however; it is not universally accepted in all cultures and political contexts, it requires external vendor expertise, and it can increase risk exposure from the perspective of personal data privacy, among other potential challenges.

The need to eliminate duplicate voter registrations has made it essential for EMBs to digitize the voter registration process, 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.[177]

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.[178]

---

[176] Air-gapped networks have no connections to outside networks (such as the internet) and are hence physically isolated.

[177] 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.

[178] Gotinga, J. (2016, April 12). *Comelec: No Biometrics in Leaked Data*. CNN Philippines. https://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html; and Tanner, A.

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.

Risk discussion: Identifiable risks include breaches or misconfiguration of online cloud storage housing voter registration databases, leading to the exfiltration of sensitive data. Malign actors could potentially target registration databases to place fake records or delete important information as well.[179] Because offline voter registration collection processes are still fairly common in most parts of the world, particularly when collecting biometric data that requires more storage capabilities, 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.

The leak of personal identifiable data is an increasing concern, both due to more mature legal frameworks protecting citizens as well as the advanced capabilities of criminal groups to use stolen data for identity theft. The risk of harm to citizens increases according to the amount of voter registration data collected – more detailed data can mean greater utility to identity thieves. Breaches can also undermine the reputation of an EMB. When voter verification equipment, such as electronic poll books, are connected to the internet, compromise could lead to voter suppression or a voting disruption.[180] 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 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.** (Note: this step may not be possible or necessary, if the voting public is able to proactively exercise functions online that must be authenticated and validated by the voter register database. For example, in the U.S. it is becoming increasingly common for voters to be able to request absentee ballots register to vote online.[181])
- **EMBs should employ designs that protect networks by using segmented protections.** This is akin to using multiple locked doorways in a long hallway, wherein each door provides an additional layer of security.
- **EMBs should use a third-party risk management process.** This means that as EMBs procure hardware, software, and services, they should formalize strategies to understand and address risk introduced by those third-party items and services. This includes the creation of policies and procedures governing vendor relationships, performing due diligence ahead of utilizing third-party services, and incorporating holistic strategies to limit identified risks.

(2016, April 22). *Mexico's Entire Voter Database Made Accessible on the Internet.* Scientific American. https://www.scientificamerican.com/article/mexico-s-entire-voter-database-made-accessible-on-the-internet/

[179] Dawood (2021) and Shackelford et al. (2017).

[180] Government Technology. (n.d.). *Digital Poll Book Failures Slowed Voting in Several States.* https://www.govtech.com/security/digital-poll-book-failures-slowed-voting-in-several-states.html

[181] Case, D. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center (E-ISAC), 388.

- **EMBs should employ a patch management strategy that ensures timely closure of known vulnerabilities via updates issued by hardware and software providers.** Making sure hardware and software have the latest updates can quickly become a complex task across larger IT infrastructures. EMBs should ensure the task is approached strategically using industry good practice to identify assets most at risk to prioritize updates while keeping track of important metrics to track and improve performance in applying patches.[182]
- As specified in earlier sections, **EMBs should implement technical controls such as encryption for data in transit and at rest**; this is particularly important for biometric data that require more storage capabilities than demographic data.
- **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.

E. 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 a risk that this personal information may become a target for various malign actors seeking to steal information for political purposes 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**.

[182] 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.

- 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.**

F. EMB COMMUNICATIONS PLATFORMS

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.

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 media 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.

G. VOTER INFORMATION AND EDUCATION

Overview and main uses of technology: The provision of voter information and education is often a continuous process. 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. Tools and technologies vary by country context; while low tech solutions such as SMS campaigns, voice bots, or radio/podcasts are still used in rural areas, most countries are now using internet content, such as websites and YouTube channels. It is worth noting the exponential increase of the use of social media across the world, as a tool that has been adopted by most election administrations.

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.[183] 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.[184]

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 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.

H. 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 voters, direct recording electronic (DRE) voting machines, optical scanners, or ballot marking devices (BMD).[185] Internet and absentee voting options are also part of this category

[183] 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 Phnom Penh Post. (2017, October 9). *NEC Facebook Hack Investigated*. https://www.phnompenhpost.com/national/nec-facebook-hack-investigated

[184] 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 International Society for Fair Elections and Democracy. (2021, September 28). *Manipulative Campaign on Facebook Regarding Election Processes*. https://isfed.ge/eng/sotsialuri-mediis-monitoringi/manipulatsiuri-kampania-Facebook-ze-saarchevno-protsesebtan-dakavshirebit; and FactCheck. (2021, September 28). *Fabricated Image of the CEC Chairperson's Decree Is Disseminated Through Social Networks.* https://factcheck.ge/en/story/39991-fabricated-image-of-the-cec-chairperson-s-decree-is-disseminated-through-social-networks

[185] As described by the Brennan Center, ballot marking devices (BMD) are tools that mark a ballot (generally a paper ballot) on behalf of a voter interacting with "visual or audio prompts provided by a computerized interface." In the United States, BMDs are often used to satisfy federal requirements for voters with disabilities to vote privately and independently; "BMDs are also able to efficiently provide ballots in alternative languages…[and] can improve the accuracy of voters' intentional markings on paper ballots, including elderly voters and those with hand tremors." See Brennan Center for Justice at New York University School of Law. (2018, May 31). *Brennan Center Overview of Voting Equipment.* https://www.brennancenter.org/our-work/research-reports/brennan-center-overview-voting-equipment. According to Verified Voting, "Most ballot marking devices provide a touchscreen interface together with audio and other accessibility features similar to those provided with DREs, but rather than recording the vote directly into computer memory, the voter's selections are indicated through a marking a paper ballot, which is then scanned or counted manually." See Verified Voting. (n.d.). *Voting Equipment: Ballot Marking Devices & Systems*. https://verifiedvoting.org/votingequipment/#row1

and, as non-supervised voting methods with a potentially high number of technological components, also have a large exposure to various cybersecurity risks.[186]

Risk discussion: Cybersecurity 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,[187] which seek to change information or votes.[188] 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) 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.[189] 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.[190] 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 compromised before it is installed in the EVM to alter votes after they are entered but before they are recorded.

Remote access to internet-based 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.[191]

Global interest in and demand for internet voting has increased with the COVID-19 pandemic. Internet voting is probably one of the most difficult technological infrastructures an EMB can choose to implement, as it touches upon the very core of the entire electoral process. Internet voting provides an opportunity to resolve some historical electoral problems – such as potential enfranchisement of voters abroad, voters with disabilities and internally displaced persons – and presents an opportunity to potentially obtain quicker results free from human errors due to counting, for example. However, it also introduces a wide range of new risks and concerns from the perspective of security, secrecy, transparency and trust.[192] Security – as well as the perception of security – should be a key consideration before implementing

---

[186] Applegate, M., T. Chanussot and V. Basysty. (2020). *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. International Foundation for Electoral Systems. https://www.ifes.org/publications/considerations-internet-voting-overview-electoral-decision-makers

[187] In cryptography and computer security, a man-in-the-middle, monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle (MITM) or person-in-the-middle (PITM) attack is a cyber attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. See: National Institute of Standards and Technology, *Glossary*.

[188] Gallagher, S. (2011, September 28). *Diebold voting machines vulnerable to remote tampering via man-in-the-middle attack.* Ars Technica. https://arstechnica.com/information-technology/2011/09/diebold-voting-machines-vulnerable-to-remote-tampering-via-man-in-the-middle-attack/; and Information Security Newspaper. (2017). *Def Con Voting Village – Hackers Easily Pwned US Voting Machines.* https://www.securitynewspaper.com/2017/07/31/def-con-voting-village-hackers-easily-pwned-us-voting-machines/

[189] 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.

[190] Hodgson et al. (2020).

[191] Although not a cyber-attack, a DOS impacted the Florida voter registration system. See Caina Calvan, B. and T. Spencer. (2020, October 7). Server Configuration Caused Florida Voter Registration Crash. https://apnews.com/article/election-2020-tallahassee-florida-elections-ron-desantis-8c986dbc04f5e5205fdcacfaa637b2af

[192] Hains et al. (2020); Springall et al. (2014); Wolchock and Halderman (2012).

internet voting. Several countries have moved away from limited internet voting programs – including the Netherlands and Norway – over security concerns.[193]

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**.[194] 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.
- **EMBs should consider security testing by independent parties**, either through code and hardware inspections, penetration testing or other evaluations.
- **The use of voter-verifiable paper audit trails (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 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.

With regards to **internet voting**, there is no standard set of mitigation strategies that are accepted across the industry. More work is needed in the following areas:

- **End-to-end verifiability** has become a requirement in theory but remains challenging to deploy in nation-wide elections. Estonia, for example, has improved the techniques to allow voters to check their votes before it is permanently recorded. After casting a ballot at a computer, each voter receives a QR code that is valid only for 30 minutes and allows the voter to check the vote from a different device (e.g., a smartphone).[195]
- **Voters' personal devices are of particular concern** for large scale electoral operations, as they are difficult to secure when not in a controlled environment.
- The **infrastructure for storing and counting votes requires special measures**, including: DDoS mitigation, to ensure ballots are received and important public facing infrastructure cannot

[193] Applegate et al, *Considerations on Internet Voting*.
[194] 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 received. If the hash values are different, it can indicate the device has been tampered with during transmission or transport.
[195] According to the Encyclopedia Britannica, a Quick Response (QR) Code is "a type of bar code that consists of a printed square pattern of small black and white squares that encode data which can be scanned into a computer system. The black and white squares can represent numbers from 0 to 9, letters from A to Z, or characters in non-Latin scripts..." See Encyclopedia Britannica. (n.d.). *QR Code*. https://www.britannica.com/technology/QR-Code

be overloaded by requests directed by malicious actors; and offline and split decryption keys to ensure the security of the votes stored.[196]

- **Blockchain technology** has been widely advertised by vendors as a solution to the security concerns of internet voting. However, it has yet to prove its benefits versus other methods of establishing a verifiable audit trail. For example, blockchain does not resolve the issue of the integrity of the vote before the ballot reaches the blockchain, it does not address the issue of voter identification, nor does it protect against DDoS attacks or APTs that would have compromised electronic voting infrastructure.[197]

I. 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. However, currently a vast majority of countries count the votes at the polling-station level. A variety of technologies may be employed at this stage, including: scanners to 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.[198] 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.[199] Hardware and software utilized at polling stations, even if 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 of the holistic risk management program.[200]

---

[196] In Estonia, the cryptographic key that decrypts the votes is split among several parties that have to physically meet to virtually "open the ballot box". Without the complete key, the votes cannot be counted.
[197] David Jefferson (2018), *The Myth of "Secure" Blockchain Voting*. Verified Voting. https://verifiedvoting.org/the-myth-of-secure-blockchain-voting/
[198] Bernhard, M. et al. (2019). *UnclearBallot: Automated Ballot Image Manipulation*. Springer International Publishing. https://www.springerprofessional.de/en/unclearballot-automated-ballot-image-manipulation/17199860
[199] Temple-Raston, D. (2021, April 16). *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack.* NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[200] Daniel, B. (2021, April 14). *System Hardening: An Easy-to-Understand Overview*. Trenton Systems. https://www.trentonsystems.com/blog/system-hardening-overview

- 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.[201] When not in use, all USB ports, WIFI and Bluetooth should be disabled.
- Ideally, the ICT systems used for the counting process should be **housed in an enclosed case and have full disk encryption enabled**.[202]
- **EMBs should establish and maintain the 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.

J. RESULTS TRANSMISSION, TABULATION AND REPORTING

Overview and main uses of technology: Tabulation of results often can take place at constituency counting centers and/or at a national results center, depending on the law in place. It is important that results be demonstrably secured to prevent questions of integrity or accuracy at each step through transmission and consolidation of results at central locations where results are aggregated and 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; web-based results software; scanned forms sent via email; 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 tactic 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.[203] Along with attacks on elections systems and websites, disinformation campaigns pose a major threat in the post-election period. Release of false

---

[201] Wilkins, R., and B. Richardson. (2013, September). *UEFI Secure Boot in Modern Computer Security Solutions*. Unified Extensible Firmware Interface Forum. https://uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf

[202] "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 Ford, A. And L. Huthinson. (2016, January 16). *Full Disk Encryption: Do We Need It?* CSO. https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html

[203] 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 Techopedia. (n.d.). *Zombie Network*. https://www.techopedia.com/definition/27201/zombie-network#:~:text=A%20zombie%20network%20is%20a,also%20known%20as%20a%20botnet

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.

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 Kremlin. 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 manipulated. The results data was changed, so that it no longer aligned with the scanned ballots in the ballot box.[204]

Mitigation strategies:

- 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.[205]

A Caveat On Tabulation Audits

As IFES has noted previously, tabulation 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. Some DREs produce a paper receipt that can be used as part of the audit trail. 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."[206]

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..."[207]

- **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

[204] European Union Election Expert Mission to Iraq. (2018). *Final Report (5 April-31 May, 24-31 July 2018).* European Union; and Wahab, B. (2018, June 11). *Recount will Test the Integrity of Iraq's Elections*. Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/recount-will-test-integrity-iraqs-elections
[205] Shein and Brown, *Risk-Limiting Audits.*
[206] Mohanty, V., et al. (2019). Auditing Indian Elections. Department of Computer Science and Engineering, Indian Institute of Technology, Madras, page 2. https://arxiv.org/pdf/1901.03108.pdf
[207] Verified Voting. (2019). *The Role Of Risk-Limiting Audits In Evidence-Based Elections*. https://verifiedvoting.org/the-role-of-risk-limiting-audits-in-evidence-based-elections/

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 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.[208] 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."[209] 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.
- **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.**[210]
- As with the IT infrastructure discussed in earlier sections, **end-to-end encryption**[211] 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**.

K. 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. Increasingly, election dispute resolution (EDR) bodies use technology as part of the complaints adjudication processes. For example, many forums accept complaints through online channels, some online portals allow the uploading of electronic evidence, hearings are increasingly being held remotely, and EMBs and EDR tribunals are also increasingly relying on electronic case management systems.[212]

Risk discussion: The EDR systems mentioned above are partially public facing systems and may contain sensitive data related to electoral contests (e.g., candidate information, voter registration data, and election results data). Cyber-attacks on the EDR process may not currently be considered to be as high of a risk to electoral processes as attacking EMB systems; however, any malicious actor with the objectives

[208] Shein and Brown, *Risk-Limiting Audits.*
[209] Vickery, C. & K. Ellena. (2020). *Election Investigations Guidebook: Standards, Techniques and Resources for Investigating Disputes in Elections (STRIDE)*. The International Foundation for Electoral Systems.
[210] Xie, T., et al. (2020). *The Untold Secrets of WiFi-Calling Services: Vulnerabilities, Attacks, and Countermeasures*. IEEE Transactions on Mobile Computing.
[211] End-to-end encryption is a term that describes the use of cryptographic encoding of data between two or more end points. Virtual private networks, for example, use end-to-end encryption to securely connect computers over the Internet.
[212] Davis-Roberts, A. (2009, January). *International Obligations for Electoral Dispute Resolution: Discussion Paper*. The Carter Center. https://www.cartercenter.org/resources/pdfs/peace/democracy/des/edr-approach-paper.pdf

of causing frustration and undermining democratic processes, would be aware of *all* public facing systems that could be easily taken offline or manipulated. Therefore, EDR bodies should take many of the same risk mitigation steps that EMBs and other electoral stakeholders take to protect their systems from cyber-attacks.

Mitigation strategies:

- As discussed above, the **legal framework must clearly provide for the regulation of election technology,** the legal requirement of maintaining a paper trail of voter intent, and provide the resources (allocating funding) and mechanisms needed for EDR bodies to ensure that their systems are both secure and transparent.
- **The law must also give EDR bodies the necessary mandate to investigate the integrity of election technology processes and outcomes through post-electoral audits** (that are clearly regulated in advance), and empower them – via experts – to perform cyber-forensics of the results chain.
- Judges, lawyers, clerks and **all actors that have access to EDR systems should receive basic cyber hygiene training** prior to any electoral event**.**
- **EDR bodies should design, maintain, and update incident response and recovery plans that include their strategy to back-up data and maintain redundant systems and procedures**. Such a plan would address backups of chain of custody records, including evidence inventory, to ensure recovery after a cybersecurity incident. **All official complaint related communications should be acknowledged, timestamped, and receipts produced with unique identifiable code** that can be traced to original documents.
- **EMBs and courts should maintain a paper-based complaint filing system and they should publish their decisions in numerous forums**, such as their websites but also official journals and newspapers, in case electronic channels are compromised or disabled.

L. 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 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.[213] 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 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."[214]

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

[213] Cybercrime Convention Committee (T-CY). (2019, July 8). *T-CY Guidance Note #9 Aspects of Election Interference by Means of Computer Systems Covered by the Budapest Convention*. Council of Europe. https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23

[214] Council of Europe. (2020). *Electoral Dispute Resolution: Toolkit for Strengthening Electoral Jurisprudence*. https://rm.coe.int/electoral-dispute-resolution/16809f0007

candidate in California.[215] 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.[216] 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.[217] 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.

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 combating electoral offenses, in line with international standards.[218]

- **It is imperative that EMBs and investigators be 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. [219]
- In the spirit of the Budapest Convention, **EMBs may also consider initiating peer platforms for information and good practice sharing, and international emergency hotlines in the realm of detecting and investigating cyber-attacks on elections**.
- Similar to the civil society context, high profile political targets will not be protected by basic cyber-hygiene practices. As demonstrated by the Pegasus leak,[220] 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.

---

[215] United States Department of Justice. (2020, February 21). *Santa Monica Man Arrested on Federal Charges of Staging Cyberattacks on the Computer System of Congressional Candidate.* https://www.justice.gov/usao-cdca/pr/santa-monica-man-arrested-federal-charges-staging-cyberattacks-computer-system

[216] Associated Press. (2020, October 23). *EU Slaps Sanctions on 2 Russians Over Germany Cyber Attack.* https://www.securityweek.com/eu-slaps-sanctions-2-russians-over-germany-cyberattack

[217] BBC News. (2018, July 13). *Twelve Russians Charged with US 2016 Election Hack.* https://www.bbc.com/news/world-us-canada-44825345

[218] Vickery and Ellena, *Election Investigations Guidebook.*

[219] Kiener-Manu, K. (n.d.). Cybercrime module 14 key issues: Information warfare, disinformation and electoral fraud. UNDOC. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html.

[220] Organized Crime and Corruption Reporting Project. (n.d.) *Politicians or Government Officials Selected for Targeting.* https://cdn.occrp.org/projects/project-p/#/professions/politician

V. OTHER ELECTION STAKEHOLDERS

Elections are not simply procedural in nature. Rather, an understanding of electoral dynamics should account for interactions between an EMB, political parties, civil society, state apparatus and media, among other important stakeholders. While IT infrastructure is used for activities and tasks across the election process, an EMB will only be able to exercise direct agency and control over some subset of that IT infrastructure. In addition, because the secure and successful execution of an election involves information flowing among stakeholders, an obvious threat vector is the information flows themselves.

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 distinctive functional units (for example an EMB, central government, civil registrar, 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. Inter- and intra-agency seams are also important to note, since coordination barriers can arise not only through adversary targeting but also due to standard organizational challenges such as managerial gaps and stovepiping of information. Since much of that information and coordination may happen via electronic information technology, cybersecurity must be a central consideration for EMBs.[221]

The prior section of this report focused on technology usage across various components of the electoral process, and steps EMBs can take to identify and mitigate risks. This section briefly discusses the concept of multi-stakeholder coordination on cybersecurity in elections. It also highlights two important electoral stakeholder groups that may be targeted by threat actors: 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 the Cybersecurity and Infrastructure Security Agency (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.

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

[221] 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).

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.[222]

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 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 promoting 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, independent 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.

In many countries, national and local CSOs play a key role in 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 cybersecurity vulnerabilities for CSO observers. This can include the insecurity of databases containing observer information (such as names, locations, email addresses, phone

[222] See, for example International IDEA's Models of Interagency Collaboration: van der Staak, S. and P. Wolf. (2019). *Cybersecurity in Elections: Models of Interagency Collaboration.* International IDEA. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

numbers). Databases containing observers' PII[223] 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.[224] Finally, the transmission of observer reports and communications via insecure 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,[225] brute force attacks (where hackers attempt to guess a password to gain entry to a CSO's internal communication systems),[226] 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 Wi-Fi networks, and instead use end-to-end encrypted messaging platforms.[227]

C. POLITICAL PARTIES

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 countries political parties have tens of thousands of members, and sometimes affiliate groups associated with the party. Political parties need to store information for all the members associated

---

[223] McCallister, E., T. Grance and K Scarfone. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information*. National Institute of Standards and Technology. Vol. 800, No. 122. https://csrc.nist.gov/publications/detail/sp/800-122/final

[224] Cybersecurity & Infrastructure Security Agency. (2013, June 24). *Alert (TA13-175A) Risk of Default Passwords on the Internet.* https://us-cert.cisa.gov/ncas/alerts/TA13-175A

[225] Cybersecurity and Infrastructure Security Agency. (2019). Phishing. https://www.cisa.gov/sites/default/files/publications/NCSAM_Phishing_2020.pdf

[226] Esheridan. (n.d.). *Blocking Brute Force Attacks.* OWASP. https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

[227] Ermoshina, K., F. Musiani, and H. Halpin. (2016, September). "End-to-End Encrypted Messaging Protocols: An Overview." In International Conference on Internet Science. Springer, Cham. pp. 244-254.

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.

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 addition to undermining their electoral efforts, researchers have also noted that targeting the private data of candidates may have a chilling effect and deter candidates from participating in elections altogether.[228] 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.[229] 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.[230] 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.[231]

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.

---

[228] Tenove et al. (2018)

[229] Whitaker, B. (2020, August 23). *How Russian intelligence officers interfered in the 2016 election.* CBS News. https://www.cbsnews.com/news/russian-hackers-2016-election-democratic-congressional-campaign-committee-60-minutes-2020-08-23/

[230] Zeit Online. (2021, March 26). *Russische Hacker Attackieren Offenbar Bundestag.* https://www.zeit.de/politik/deutschland/2021-03/cyberangriff-russland-hacker-bundestag-ghostwriter-geheimdienst-gru-cyberwar

[231] 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.

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.[232] The information that has emerged from the leak shows that governments can 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.

VI. CONCLUSIONS

The analysis in this report illustrates the way electronic information systems are heavily utilized across the electoral process. 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.

We recognize, however, that many EMBs may not currently be sufficiently resourced or positioned to enact such mature cybersecurity programs. The risk management frameworks used 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, 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

[232] 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 Corruption Reporting Project) aims to expose how Pegasus is being exploited. See Organized Crime and Corruption Reporting Project (n.d.). The Pegasus Project. https://www.occrp.org/en/the-pegasus-project/

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 process. 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.

ANNEX: 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 Cybersecurity 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.

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, L., Cordova McCadney, L. 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.

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.

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

D. ACADEMIC LITERATURE

Shackelford, S., Schneier B., Sulmeyer, M., Boustead, A., Buchanan, B., Deckard, A. N. C., Herr, T., Smith, J. M. (2017). Making Democracy Harder to Hack. 50 U. Mich. J. L. Reform 629.

Dawood, Y. (2021). Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats. Election Law Journal: Rules, Politics, and Policy, 20(1), 10-31.

Garnett, H. A., & James, T. S. (2020). Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. Election Law Journal: Rules, Politics, and Policy, 19(2), 111-126.

Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy. Research Report, Centre for the Study of Democratic Institutions, University of British Columbia.

Hodgson, Q. E., Brauner, M. K., Chan, E. W. (2020). Securing U.S. Elections Against Cyber Threats: Considerations for Supply Chain Risk Management. Santa Monica, CA: RAND Corporation.

Fidler, D. P. (2017). Transforming Election Cybersecurity. Articles by Maurer Faculty. 2547.

Henschke, A., Sussex, M., & O'Connor, C. (2020). Countering foreign interference: election integrity lessons for liberal democracies. Journal of Cyber Policy, 5(2), 180-198.

Kasongo, E., Bernhard, M., & Bronk, C. (2021). Tales from the Trenches: Case Studies in Election Cybersecurity Preparedness in Texas. E-Vote-ID 2021, 113.

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).

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.

E. 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.).

F. OTHER REPORTS

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