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