Cybersecurity in Elections

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

October 2018

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
· 30 Years ·

Cybersecurity in Elections:
Developing a Holistic Exposure and Adaptation Training (HEAT) Process for Election Management Bodies

October 2018

Katherine Ellena and Goran Petrov
International Foundation for Electoral Systems

Contributors:

Russell Bloom
Gina Chirillo
Dr. Staffan Darnolf
Ronan McDermott
Dr. Beata Martin-Rozumiłowicz
Erica Shein
Chad Vickery
Mike Yard

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

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

Preface

The International Foundation for Electoral Systems (IFES) has worked for more than 30 years in over 145 countries to support the right to free and fair elections worldwide. Securing that right once it has been established is a major part of our work. As technology changes, countries and their election management bodies (EMBs) must change how they conceive of security. Bad actors, whether foreign or domestic, use technology to enhance their reach and the damage they can inflict. Battles for the integrity of elections are increasingly waged in cyberspace, and one small flaw in technology, or in the way it is used, can jeopardize an election. Hence, strengthening cybersecurity in democracies is increasingly important, and IFES is continuing to expand our support to electoral cybersecurity globally.

Even as cyberattacks become more frequent, electoral processes are becoming increasingly reliant on the kinds of technology those attacks exploit. Elections increasingly depend on technology such as digital voter rolls and election results, biometric voter registration, and electronic voting machines. Countries are continuing to adopt these technologies, so the need for an effective framework for protecting against cyberthreats has never been greater. This cannot be an afterthought in the electoral process. Rather, a discussion around the ever-changing electoral threat environment should inform the public procurement process for any election technology. To do otherwise is to risk the possibility that actual or perceived vulnerabilities are exploited to undermine the credibility of the process.

The balance between transparency and security is perhaps the central issue in cybersecurity in elections. While technology needs to be sufficiently opaque to bad actors, the public can quickly lose trust in any system that is a “black box” to non-experts. Securing this technology means more than just strong software and hardware – it also means securing the human, political, legal and procedural aspects of an election. A technology can only be as secure as the processes and the people around it. Building on case studies and an extensive literature review, IFES has turned its lessons learned into a methodology to assist EMBs in their defense against cyberattacks on the democratic process. The methodology presented in this paper, called the Holistic Exposure and Adaptation Testing (HEAT) process, is a holistic framework for understanding and responding to threats to electoral cybersecurity.

Drawing on an extensive literature review and our technical expertise, IFES developed this framework with the shifting technological landscape in mind. The nature of technical innovation means that cyberattacks cannot be wholly prevented, but they can and should be anticipated as much as is possible. The HEAT process is designed to support EMBs in assessing and protecting against cyberthreats.

Protecting the fundamental right to free and fair elections now requires a cybersecurity strategy and infrastructure. IFES wrote this paper to that end and will continue defending democratic electoral processes from cyber interference in support of citizens’ right to political participation and representation.

William R. Sweeney, Jr.
IFES President and CEO

Contents

I. Introduction

In June 2017, 100 election experts from across the United States penned an open letter to Congress noting that many jurisdictions were "inadequately prepared to deal with rising cybersecurity risks."[1] This concern is echoed globally, as increasing reliance on complex technology-based systems in electoral processes has left troves of sensitive information potentially vulnerable to adversaries.[2] Experiences in several recent elections around the world highlight threats to cybersecurity, as well as how the implementation of certain electronic data management technologies can impact post-election disputes.[3] However, many election management bodies (EMBs) lack the capacity, resources, or appropriate framework to test whether their data management systems are secure from these vulnerabilities, and to put measures in place well in advance of elections to protect data integrity.

Cybersecurity[4] should be considered and implemented at the inception phase of building or upgrading any technology-based election system, as a key component of digitizing specific elements of election administration. At the same time, international good practices around cybersecurity and open data require EMBs to act transparently and to ensure election results are verifiable and can ultimately be accepted by the electorate. Therefore, it is important to protect both cybersecurity and transparency in the electoral context – a challenge that is particularly unique to EMBs.[5]

Beyond striking this balance, election administrators must focus on cybersecurity as an ongoing and ever-changing concern. As soon as cybersecurity good practices are developed, they may become outdated, because technology moves forward very quickly, as does the technical expertise of those who seek to find and exploit its vulnerabilities. While it is important to learn from experience, rapid technological innovation means that EMBs should endeavor to secure the *next* election, not focus on vulnerabilities in the *last* election. This means identifying potential future vulnerabilities, not only addressing issues that have been identified or exposed in the past.

[1] "Election Integrity Open Letter to Congress," National Election Defense Coalition, https://www.electiondefense.org/election-integrity-expert-letter/.

[2] Reuters, "Two 11-year-olds altered election results in hacker convention's replica of U.S. voting system," *CBC,* August 14, 2018, https://www.cbc.ca/news/technology/def-con-hacking-convention-voter-village-1.4784803.

[3] For example, electronic transmission of results at the polling station level or maintenance of national biometric voter registration databases, but also penetration of less high-profile databases such as personnel records for ad hoc staff, that could undermine the public's confidence in the EMB and its capacity to secure more sensitive databases.

[4] A note on definitions: In this paper, IFES uses the terms "cybersecurity," "data security" and "data protection" interchangeably, in line with ISO standards and academic literature. See, for example, Basie Von Solms, Rossouw von Solms, "Cyber security and information security – what goes where?", Information & Computer Security, https://doi.org/10.1108/ICS-04-2017-0025, which offers a definition that: "Cyber Security [is] part of Information Security, which specifically focuses on protecting the Confidentiality, Integrity and Availability (CIA) of digital information assets against any threats, which may arise from such assets being compromised via (using) the Internet."

[5] For example, other agencies such as defense, or institutions such as banks or insurance agencies, can focus primarily on cybersecurity without the same transparency concerns.

It also means looking at cybersecurity holistically, as one type of vulnerability may be addressed in isolation while another is exploited instead. Or, different types of cybersecurity exposure may compound to produce a unique vulnerability that can result in significant problems, whether through malpractice (negligence or mistake) or fraud (deliberate exploitation).[6] While existing guidelines on cybersecurity, discussed in the literature review below, provide sound guidance on mitigating technological exposure in elections (for example, by ensuring sound cyber hygiene practices and implementing two-factor authentication), they may not consider other types of exposure, such as restrictive laws, weak procedures or untrained staff, that can undercut cybersecurity frameworks and lead to breakdowns in the electoral process or in public trust of electoral outcomes.

Types of Cybersecurity Exposure in Elections

Technology Exposure – *for example, through hacking or system failure*

Human Exposure – *for example, through poorly trained or malevolent officials using data systems*

Political Exposure – *for example, through improper influence over the procurement process for election technology*

Legal Exposure – *for example, through poorly drafted or manipulated laws that restrict EMB independence or leave the process vulnerable to litigation*

Procedural Exposure – *for example, through poorly designed procedures that create vulnerabilities in how data is managed*

Given all these considerations, how can EMBs secure systems from technical vulnerabilities that leave them exposed and may lead to post-election challenges, while at the same time protecting principles of open data and transparency?

In this paper, the International Foundation for Electoral Systems (IFES) outlines strategies for EMBs to strengthen their technology and procedures to resist vulnerabilities, by following what we have termed a Holistic Exposure and Adaptation Testing (HEAT) process. While no electoral process or technology is infallible, the HEAT process aims to secure automated or digitalized electoral processes – as far as possible – against unanticipated threats, illicit incursions, system failures, or unfounded legal challenges.

As the name suggests, the HEAT process focuses on the types of exposure an EMB may face when implementing different types of technology systems (technology, human, political, legal and procedural

[6] IFES has defined these terms further in Chad Vickery and Erica Shein, *Assessing Electoral Fraud in New Democracies: Refining the Vocabulary*, May 2012, http://www.ifes.org/sites/default/files/assessing_electoral_fraud_series_vickery_shein.pdf. Electoral fraud differs from electoral malpractice along several key dimensions. The range of possible actors is wider for fraud, as it can include any person or group with a stake in the election result. This may include voters, political parties, state officials with election-related duties, candidates and the media, in addition to election workers. Malpractice, on the other hand, is largely analyzed in the context of election officials (permanent and ad hoc staff), though other actors (e.g., political parties, the media) can breach their duty of care as it relates to codes of conduct, guidelines, or internationally accepted best practice. The nature of the action and the presence of intent is most significant: fraud is committed deliberately and with intent to interfere with the electoral process (manifested as either an action or an omission, in the case of an actor with official election responsibilities), while malpractice results from carelessness or neglect.

exposure, as summarized in the text box). This process encourages a more holistic assessment of what could go wrong in data and technology management and allows the EMB to identify strategies to reduce or eliminate different types of exposure in a systematic manner.

Because the HEAT process seeks to provide a holistic approach to cybersecurity in elections, we have drawn lessons from international principles, election cybersecurity case studies, risk-mitigation methodologies and technology-related election court judgments. The proposed process is also guided by international best practices on data management and cybersecurity, as well as transparency, open data and privacy.

A thorough HEAT process, as described in this paper, has significant time and cost implications. However, without such a process in place, an EMB may experience an electoral crisis that far exceeds the time and resources invested in such a risk-mitigation process. It is important to note that a HEAT process is only suitable for the earlier part of the electoral cycle when there is significant time for the EMB to implement measures to mitigate identified deficiencies. While the HEAT process itself may be achievable in a short time period, it is often the case that cyber vulnerabilities cannot be addressed by "quick fixes," but require significant lead time to address properly. For example, if certain legal or procedural vulnerabilities are revealed, several months or more may be required to draft or pass amendments, or to adjust procedures and then train and publicize new procedures effectively. If a HEAT process is conducted and reveals vulnerabilities too close to an election to be able to rectify, this could then have an adverse effect on stakeholder confidence in the electoral process.[7] This is particularly true in environments with pre-existing low trust.

This paper outlines the existing literature on cybersecurity and data protection in elections, including international standards, good practice guidelines, cybersecurity frameworks, election observer guidelines, and jurisprudence. This literature is then applied to discuss the various types of exposure EMBs may face when implementing technology and seeking to protect data and data processing in elections. This application is important, as while much of the standard-setting is taking place in North America and Europe, in IFES' experience many developing democracies outside of these regions are also considering and using election technologies. Finally, the paper introduces the IFES HEAT process as a holistic tool for identifying and mitigating different types of cybersecurity exposure in elections.

II. Literature Review

a) International and Regional Standards for Cybersecurity in Elections

International standards for elections provide the basis for assessing the introduction of technology into the electoral process. Any introduction of technology must promote core election principles, such as

[7] The Venice Commission's *Good Practice in Electoral Matters*, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e, includes a provision that the fundamental elements of the election legislation should not be fundamentally amended one year prior to a forthcoming elections.

transparency and accountability of the process, as well as integrity and verifiability of election results. On the other hand, as societies evolve and technologies advance, international institutions are continually updating and refining standards for cybersecurity, transparency, open data, and privacy. These evolving standards stem from – and must adhere to – fundamental political rights established by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[8]

Beyond these universal instruments, international organizations and governing bodies are increasingly establishing international standards on the conduct of elections in which any election-related data is stored digitally. Although not the first forum to establish guidelines on data management, recognized international standards are summarized in the United Nations (UN) General Assembly Guidelines for the Regulation of Computerized Data Files.[9] Adopted by the General Assembly in 1990, these guidelines provide broad principles of data management that place responsibility for data on those persons who collect it, specifically requiring that data collectors be responsible for ensuring that the data is accurate, transparently and lawfully collected, properly restricted to avoid discrimination, securely stored, and lawfully disseminated.[10] 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."[11] These guidelines define the principle of security as taking appropriate action to "protect the files against natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses."[12] Though the guidelines do not explicitly mention election technology, they have implications for electronic data management in electoral processes and outline protections that should apply to the full range of stakeholders involved in the electoral process – voters, candidates, election officials, among others – whose data may be collected.

There are additional standards for the introduction of technology in voting or vote-counting processes specifically. Most notably, the Council of Europe's 2017 e-voting standards place specific responsibility on EMBs for the "availability, reliability, usability and security of the e-voting system."[13] 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

[8] Article 21 of the UDHR states that the will of the people "shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or be equivalent free voting procedures."

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

[10] Ibid.

[11] Ibid., sec. B.

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

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

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."[14]

Some countries establish their own voluntary standards or legislation. For example, the U.S. Electoral Assistance Commission maintains a set of voluntary guidelines to help election authorities test whether their systems meet certain functionality, accessibility and security standards. Many U.S. jurisdictions have adopted these standards as obligatory.[15] Certification of election technologies has also 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.[16]

The privacy of the individuals whose data is collected is another integral aspect of data management that has become particularly prominent with the recent passage of the European Union's (EU) General Data Protection Regulation (GDPR),[17] which went into effect in May 2018. This regulation governs personal data of EU residents that companies and organizations collect, store or process, and requires more openness about what data they have and who they share it with.[18] The UN has adopted various general resolutions on data privacy[19] 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.

For the sake of transparent elections, it is important to allow access to certain types of data to voters, political parties, and civil society organizations. For example, access to preliminary voter lists is important in order to verify details and to challenge registrants who are not eligible, and access to final voter lists is important so these can be used by party agents on Election Day and for voters to know which polling station to go to. Limitations on data access are typically imposed, such as limited access for political parties to the full voter register or its signed version.[20] In 2011, 75 countries signed the Open Government Declaration, committing themselves to advancing transparency and openness within

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

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

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

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

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

[19] 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 December 18, 2013 and 69/166 of December 18, 2014, as well as Human Rights Council resolutions 28/16 of March 26, 2015, on the right to privacy in the digital age and 32/13 of July 1, 2016 on the promotion, protection and enjoyment of human rights on the Internet.

[20] Ed. Michael Yard, *Civil and Voter Registries: Lessons Learned from Global Experiences,* IFES, 2011, 15.

government.[21] The declaration includes a provision for increasing access to and use of new technology in order to make government practices transparent, secure online spaces and platforms, and provide "alternative mechanisms of civic engagement."[22]

The Open Government 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."[23] These standards will be essential when implementing voting and counting technology, where individual information must be securely and transparently stored and checked to ensure the validity of both the voters and the votes.

b) Best Practice Guidelines for Implementing Election Technology

Improper management and implementation of technology can discredit an entire electoral process, leading to public disenchantment with elections and even violence. Although there are a variety of different principles for data collection and management, there is no single set of good practice guidelines for their implementation. A substantial number of intergovernmental and international non-governmental organizations, including the Council of Europe, European Commission, IFES, International IDEA, the National Democratic Institute (NDI), and the Organization for Security and Co-operation in Europe's Office for Democratic Institutions and Human Rights (OSCE/ODIHR), among others, have contributed guidelines and handbooks on election technologies.

There are three recent publications that connect cybersecurity and elections. They are all valuable contributions in advance of upcoming elections around the world and the use of technology therein. In February 2018, the Center for Internet Security (CIS) published *A Handbook for Elections Infrastructure Security*, which establishes election system risks and how to mitigate them through a detailed use of good practice that county or state election administrators could implement.[24] Academic institutes such as the Harvard Kennedy School's Belfer Center have also contributed to the literature in this space, with a *State and Local Election Cyber-Security Playbook*, that is designed for U.S. election officials but can also

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

[22] Ibid.

[23] Ibid.

[24] Calkin et al., *A Handbook for Elections Infrastructure Security*, Center for Internet Security, 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

be used in wider contexts.[25] 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). Most recently, in July 2018, an EU Cooperation Group[26] published a *Compendium on Cyber Security of Election Technology* that aims to systemize the cyber concerns and threats across the European continent and offers myriad experiences accumulated from EU member states' elections in case studies.[27]

IFES argues that one of the first steps in implementing election technology is to weigh the costs and benefits of adopting a particular tool.[28] IFES has found through global experience that EMBs or governments often focus on security concerns during the collection of data, and focus less on how the data will be processed, transmitted and stored. Regardless of country context, this step should always include the input of a diverse group of stakeholders, such as election officials, government leaders, political party leaders, and civil society organizations, including special needs groups. This assessment also provides an opportunity to identify the problems in the electoral process that a particular technology can help solve. IFES' own work on guidelines states that "a specific technology should only be considered if there is a specific problem that the technology can address."[29] It is important that there be a clear need for the technology, and that technology is not introduced for technology's sake. The technical and financial feasibility, potential benefit, and likelihood of acceptance by stakeholders of the new technology should be evaluated before testing whether the technology is a good fit.[30] The common practice of procuring election technologies from private vendors, for example, brings potential benefits, such as world-class technology expertise and global experience, but also risks. IFES, the European Commission, and the UN Development Programme (UNDP) all note the risk of private vendors having control over EMB operations once the technology is in place, with EMBs unable to switch technology again without incurring huge costs.[31] Security vetting of private contractors can also be a challenge.

IFES has found through global experience that EMBs or governments often focus on security concerns during the collection of data, and focus less on how the data will be processed, transmitted and stored.

[25] Harvard Kennedy School's Belfer Center, Defending Digital Democracy Project (D3), *The State and Local Election Cyber-Security Playbook*, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.
[26] Comprising experts from the EU member states, the European Commission and ENISA.
[27] EU NIS Cooperation Group, *Compendium on Cyber Security of Election Technology*, July 2018, https://www.ria.ee/public/Cyber_security_of_Election_Technology.pdf.
[28] Ben Goldsmith and Holly Ruthrauff, *Implementing and Overseeing Electronic Voting and Counting Technologies,* IFES and NDI, 2013, 23-24.
[29] Michael Yard, ed., *Direct Democracy: Progress and Pitfalls of Election Technology*, IFES, 2010, 20.
[30] Ben Goldsmith, *Electronic Voting and Counting Technologies,* IFES, 2011, 13.
[31] European Commission and UNDP, *Procurement Aspects of Introducing ICTs solutions in Electoral Processes,* 2010, 73; and Yard, ed., *Direct Democracy: Progress and Pitfalls of Election Technology*, International Foundation for Electoral Systems, 112.

The electoral legal framework may present a challenge for the introduction of new technology in the electoral process. The relevant legal provisions may reside in three locations: "the constitution, if there is one, the laws relating to elections (or articles in general laws related to elections, such as for example, the criminal code), and the secondary legislation (such as regulations, rules and procedures often passed by EMBs)."[32] In some cases, legislation governing these technologies may be found in areas outside of elections, such as regulations on data protection.[33] 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."[34] 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."[35]

In addition, the country's specific election system must also be considered before implementing new election technology. For example, before using new technology for voter registration, it is important to know who registers voters (the EMB, another government agency, or another organization), who collects data on voters, how that information is shared with the EMB (if the EMB does not collect the data), and who owns the data.[36] New technology typically requires additional human capital considerations, such as stronger information technology (IT) skills and experience. Many election staff often lack the skills to manage new technology without training.[37] In Kosovo in 2010, local staff were found to need two electoral cycles' worth of training before they would have the IT skills and experience necessary to run the relevant technology on their own.[38] This highlights the security risks around poorly equipped technology users who may be easy targets for malware on individual terminals that are connected to a wider system.

An appropriate timeframe for procurement, implementation, testing, and training is also a decisive factor in determining whether to use a new technology. Timelines for ensuring a smooth transition to new technology will vary by country and electoral cycle. EMBs should have a clear plan, from the initial determination of the merits of the technology to the electoral process through final implementation. Introducing new technology too quickly can fail to build public trust and can lead to technical issues, further eroding trust in the process.[39] A fundamental part of this process that is often not adequately 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

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

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

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

[35] Council of Europe, *Guidelines on Transparency of E-enabled Elections,* 2011, 5. (source no longer found)

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

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

[38] Ibid., 42.

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

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 on" to an existing system or platform.

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.[40] If public trust in the electoral process is already low, introduction of a new system may cause public unrest.[41] Rather, technology should be introduced at a stage when all electoral stakeholders enjoy significant trust in the process, rather than attempting to use technology to mask the problems. In terms of confidence-building measures, IFES has previously noted that, while fully open source code for technology platforms may not be necessary, it is the more preferable option to support transparency and public trust.[42] A growing number of governments are requiring open source technologies, which can aid with re-use, integration, and standardization, while also making the technology more sustainable and cost-effective. Open source solutions are also inherently transparent, which can improve credibility with stakeholders and avoid vendor or implementer lock-in or conflict of interest. Should open source code not be used, IFES has noted that "experts representing key electoral stakeholders (political actors and civil society) should be allowed sufficient access to review the source code and should not be restricted in reporting their analysis of its content by the use of any non-disclosure agreements (NDAs)."[43] In cases where open source technologies are not or cannot be used, NDAs should be pre-negotiated as part of the procurement process to protect the intellectual property of the technology providers and to ensure that critical stakeholders, such as political parties, observers, and election commissions, have access to the code in order to rigorously test the security and functionality of the technology and maintain minimum levels of public trust.

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, which is equally important. 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."[44] Specific tools that provide independent ways to test the system, such as voter verified paper audit trails (VVPATs) and post-election audits of technology systems, are also a good means to gain public trust and secure against fraud.[45] Public communication around contingency planning is also

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

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

[42] Ben Goldsmith and Holly Ruthrauff, *Implementing and Overseeing Electronic Voting and Counting Technologies,* IFES and NDI, 2013, 175-176.

[43] Ben Goldsmith and Holly Ruthrauff, *Implementing and Overseeing Electronic Voting and Counting Technologies,* IFES and NDI, 2013, 175-176.

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

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

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.

c) Cybersecurity Instruments and Frameworks

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

Several high-level policy institutes have developed cybersecurity frameworks to systematically address cyberthreats and vulnerabilities in any complex system. These organizations include the U.S. Computer Emergency Readiness Team (US-CERT),[48] NIST,[49] the information systems non-profit ISACA,[50] and the International Organization for Standardization (ISO).[51] In the absence of election-specific cybersecurity standards, these general frameworks may be useful for EMBs.

Cybersecurity frameworks are typically organized using a functional approach (that is, breaking down processes into functions). NIST, together with US-CERT,[52] identified a functional approach in its framework in five steps that is now widely used within the cybersecurity community: identify, protect, detect, respond, and recover.[53]

[46] "Budapest Convention and related standards," Council of Europe, https://www.coe.int/web/cybercrime/the-budapest-convention.

[47] The original ransomware attack known as "Petya" held hostage data from several companies and demanded a ransom to release it. A number of cybersecurity analysts maintain that the newer versions were instead aimed at causing damage. Olivia Solon and Alex Hern, "'Petya' ransomware attack: what is it and how can it be stopped?" *The Guardian,* June 28, 2017, https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

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

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

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

[51] ISO, https://www.iso.org/home.html.

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

[53] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* ver. 1.1, 2018, 3, https://www.us-cert.gov/ccubedvp/cybersecurity-framework.

- Identify (develop organizational understanding to manage risk),
- Protect (develop/implement safeguards),
- Detect (develop/implement activities to recognize if an event is related to cybersecurity),
- Respond (develop/implement actions to contain the impact of a cybersecurity event) and

The US-CERT framework is detailed on the comprehensive NIST website. 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 best practices for employees and general frameworks. ISACA provides a framework for information systems security audits[54] and a framework for balancing the risks and benefits of IT.[55] 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.[56]

The EU Agency for Network and Information Security (ENISA) and ISO have identified critical cyberthreats that must be addressed. ISO's cybersecurity guidelines, which were 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.[57] While some are more directly relevant to EMBs than others, all could be used to undermine the security and legitimacy of the electoral process. ENISA identified threats as diverse as information leakage, such as in the 2017 French elections, cyber espionage, such as the Russian involvement in the 2016 U.S. elections, ransomware, and insider threats.[58] The diverse landscape of threats from inside and outside an organization demonstrate the need for comprehensive and systematic cybersecurity protection.

d) Election Observer Guidelines

As well as introducing new operational and security considerations, emerging election technology has also changed the observation of elections. When observation missions are unprepared to observe, analyze, and report on the use of new technology, the legitimacy of elections can be undermined by a lack of effective observation or inaccurate observations, especially in the event of disputed results. This can be particularly true for citizen observation missions that may lack the methodologies or capacity to properly observe technology processes in elections. One example of this is the 2017 Kenyan elections, when the opposition claimed technological malfeasance and manipulation had cost them the election.[59] Citizen observers were the only ones able to verify the counting and results tabulation process, but the

- Recover (develop/implement activities related to restoring capabilities if systems were impacted and increase resilience).

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

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

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

[57] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27005:2011,* 2011; ENISA, *ENISA Threat Landscape Report 2017,* 2018.

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

[59] "Kenya opposition leader Raila Odinga claims election fraud," *Financial Times,* August 9, 2017, https://www.ft.com/content/2f795986-7cda-11e7-ab01-a13271d1ee9c.

elections ultimately were annulled over alleged irregularities in electronic results transmission and the process for final certification of results – an aspect of the electoral process that was more difficult for both citizen and international observer groups to observe.[60]

Some international election observation organizations have published handbooks on how to observe technology in elections. These documents provide future observation teams with election technology standards and best practice guidelines. The consensus among these groups favors more technical skills for core teams, longer and earlier missions, and closer observation of election technology – including during the development of specifications and the procurement stage. The Carter Center's *Handbook on Observing Electronic Voting* recommends having at least two members of a core observer team with technical skills, ideally with a combination of electoral experience and technological or computer science skills. These "e-voting experts" should have five to ten years of relevant experience.[61] Core team members without a technical background need additional training to evaluate the technical aspects of the electoral process. The Organization of American States (OAS) recommends that a "core group" of technical staff and specialists, along with long-term observers, conduct an analysis of the technology to be used in the upcoming elections. The results should be used to determine the training needed for short-term observers.[62]

New technology requires extra preparation on the part of election observation missions (EOMs). According to The Carter Center, EOMs should start as early as possible, typically four to six months before an election, and stay until any dispute resolution has finished.[63] NDI recommends observer involvement at every stage of the technological adoption process, including developing specifications for hardware and software, testing the technology, and reviewing training manuals and attending training sessions for EMB employees.[64] The Carter Center, ODIHR and the OAS provide a questionnaire for observers monitoring new election technology; the OSCE has a checklist of questions in their *Handbook for the Observation of New Voting Technologies*.[65] This demonstrates that observer groups are adapting to the new requirements that election technology presents, although funding and resources can be a challenge in supporting longer-term and more technical observation.

Apart from direct observation of key events, such as for example tabulation of election results as well as interviews with EMBs, election observers should be equipped to evaluate and report on testing and auditing, and certification, if any, of any election process that involves new technology.

[60] Julia Brothers, "Using Open Data to Verify Information in Elections," *NDI*, March 2018, https://www.demworks.org/using-open-data-verify-information-elections.
[61] The Carter Center, *Observing Electronic Voting,* (Georgia: 2012), 5.
[62] Gustavo Aldana, et al., *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*, OAS, 8.
[63] The Carter Center, *Observing Electronic Voting,* 2012, 6-7.
[64] Vladimir Pran and Patrick Merloe, *Monitoring Electronic Technologies in Electoral Processes,* NDI, (Washington, DC: 2007), 35-41.
[65] The Carter Center, *Observing Electronic Voting,* 2012, 41-65; Aldana, et al., *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*, 33-35; OSCE, *Handbook for the Observation of New Voting Technologies,* (Warsaw, Poland: 2013), 70-71.

e) Case Law

Several recent cases in national courts have provided various precedents on cybersecurity in elections centered on the following issues: implementation and transparency of technology in Kenya; electronic voting machines (EVMs) in India, Germany, and Finland; e-voting in Estonia and Austria; and cybersecurity in the Philippines, all of which are discussed below. Together, the cases highlight the importance of a verifiable paper trail for the voting and counting process, transparent tabulation and certification of results, clear procedures and instructions for using technology, equality among voters, and the importance of having cybersecurity policies and practices in place.

Implementation and Transparency of Election Technology

In its judgment annulling the August 2017 Kenyan presidential elections, the Supreme Court ruled that the Independent Electoral and Boundaries Commission (IEBC) had failed to adhere to legal requirements for "free and open elections." The election results were finalized and announced based on information from tabulated results forms (34B) that came from centralized tallying centers, instead of waiting until the IEBC received all original results forms (34A) from individual polling stations. The court focused on the IEBC's failure to provide full access to its servers and server logs and its failure to provide a plausible explanation for results released based on incomplete information. The court stated it "had no choice" but to accept the petitioners' claim that either the servers were infiltrated and the data compromised, or the IEBC itself had intentionally or unintentionally compromised the data.[66] Multiple errors in implementing technology were referenced in the decision, including interruptions on data mobile coverage without an adequate backup plan and discrepancies between results published on the website and official results released when compared to the breakdowns of results transmitted from polling stations to the National Tallying Center.

Use of Electronic Voting Machines (EVMs)

Courts in India, Germany and Finland have all ruled on EVMs, focusing on the use of VVPATs to authenticate results, voting technology that is understandable to the average voter, and clear instructions for EVMs, respectively.

In its judgment of October 8, 2013, the Supreme Court of India directed the government to fund the gradual phase-in of VVPATs, agreeing with the petitioner that a paper trail is a vital security measure for e-voting. Although the Indian Election Commission (IEC) was able to print records from their EVMs with a decoder device, the court ruled that VVPATs were also necessary. The IEC claimed that it had tested VVPATs in field trials and had not yet adopted them on the basis of those trials. The court noted that "[f]rom the materials placed by both the sides, we are satisfied that the 'paper trail' is an indispensable

[66] See section 279 of *Odinga and Musyoka v. IEBC et al. (*Supreme Court of Kenya 2017): "The IEBC in particular failed to allow access to two critical areas of their servers: its logs which would have proved or disproved the petitioners' claim of hacking into the system and altering the presidential election results and its servers with Forms 34A and 34B electronically transmitted from polling stations and CTCs."

requirement of free and fair elections. The confidence of the voters in the EVMs can be achieved only with the introduction of the 'paper trail.'"[67]

Following the 2005 parliamentary (*Bundestag*) elections, the Federal Constitutional Court of Germany ruled on two complaints about the use of computer-controlled voting machines. Complainants alleged that two laws that had been drafted, and the specific EVMs used, violated the principle of the public nature of elections, which means that all essential steps of an election "are subject to the possibility of public scrutiny."[68] The complainants moved to invalidate the elections and to repeat them with voting slips and ballot boxes. The principle of equality was also alleged to have been violated by the different treatment of voters who used voting slips and voters who used EVMs. The court ruled that one of the laws in question did permit voting machines without effective monitoring of voting or results and was therefore unconstitutional. It found that the EVMs used were also incompatible with the public principle; votes were recorded only on an electronic storage medium, so voters could not verify their votes, and could only see that the machines had registered a ballot. No procedure should render the voter unable to verify "whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast assigned and counted."[69] The court did not dissolve the *Bundestag*, saying that without evidence of manipulation, or evidence that results would have been different without the EVMs, there was no sufficient reason to invalidate the elections. The public interest "in the protection of the status quo of the people's representation composed in trust in the constitutionality of the Federal Voting Machine Ordinance outweighs the election errors that have been ascertained."[70]

EVMs were introduced in Finland through a pilot project in the 2008 municipal elections. E-voting was an option at polling stations in three municipalities, and voters there had a choice between traditional and e-voting. Voters used a voting card to cast their vote, but instructions on the card were incomplete. Accordingly, nearly two percent of e-votes were not recorded. In its decision on a subsequent election petition, the Supreme Administrative Court found that both the instructions on the cards and the EVMs used were inadequate, and annulled the elections.[71] Elections were then re-held using only traditional voting. The Council of Europe's observation report concluded that universal suffrage, especially the right to vote and the right to be elected, had been violated.[72]

Use of Internet Voting or Electronic Voting (E-Voting)

E-voting has featured in several major court decisions, most notably in Estonia and Austria. In 2005, the Estonian Parliament (*Riigikogu*) passed an amendment allowing e-voters to change their vote on the

[67] *Swamy v. Election Commission of India* (Supreme Court of India 2013).
[68] *Judgment of the Second Senate of March 3, 2009, 2 BvC 3/0* (Federal Constitutional Court of Germany).
[69] Ibid.
[70] Ibid.
[71] Sections 2.42 and 2.5 of *KHO:2209: 39* (Supreme Administrative Court of Finland).
[72] Kieth Whitmore, *Information Report on the Electronic Voting in the Finnish Municipal Elections*, Council of Europe, 2008, 3.

internet an unlimited number of times during advance polling. E-voters could also cast one paper ballot as their final vote, either in the advance period or on the day of the polls. The president of Estonia challenged the amendment in the Supreme Court, claiming that it gave e-voters an unfair advantage, violating the principle of uniformity in § 156(1) of the Estonian Constitution, interpreted as all having an equal possibility to affect the voting results. The president did not contest e-voting itself, only the ability for anyone e-voting to change his or her vote.[73]

The amendment was ruled constitutional and in line with the Council of Europe standards of e-voting. Estonia uses a mandatory ID card to verify identity in e-voting, so no legal obstacles were created. Voters already used different means to vote, such as postal voting, and did so in different situations, meaning voting was already not strictly uniform. The principle of one vote per voter was guaranteed by an electronic version of the double-envelope system used in advanced voting: voters approve their e-votes by digital signature, pairing personal data with the encrypted vote. The two were not separated until after polls closed on Election Day, ensuring that no voter could vote twice. Voters' information could not be transferred together into the computer that did the counting, guaranteeing secrecy. Each subsequent vote replaced the last, preventing voters from using multiple channels to cast multiple votes.

The court noted that a possible violation of the right to equality is only unconstitutional if it is disproportionate to the "weight of the aims pursued."[74] The aims of increasing participation in elections and modernizing voting practices were considered legitimate (although it is worth mentioning that the amendment did not actually increase turnout, and that comparative studies generally have shown that the use of technology tends not to influence turnout).[75] Further, the court found that using e-voting without allowing voters to change their vote may open this process up to possible intimidation, as internet voting is used in an uncontrolled environment, unlike the controlled environment of a polling station, where it is difficult to guarantee secrecy and freedom from intimidation.

The Austrian Constitutional Court ruled on remote e-voting following the 2008 Austrian Student Association elections, in which e-voting was introduced for the first time. Two political parties in the election brought complaints against the election and the regulations governing it. The court did not

[73] *Constitutional judgement 3-4-1-13-05* (Supreme Court of Estonia).

[74] Ibid.

[75] *See, e.g.,* Kristjan Vassil and Till Weber, "A Bottleneck Model of E-Voting: Why Technology Fails to Boost Turnout," *New Media & Society* 13, no. 8 (2011), 1336-1354; Karel Sál, "Remote Internet Voting and Increase of Voter Turnout: Happy Coincidence or Fact? The Case of Estonia," *Masaryk University Journal of Law and Technology* 9, no. 2 (September 30, 2015): 15-32; Harald Baldersheim, Jo Saglie, and Signe Bock Segaard, "Internet Voting in Norway 2011: Democratic and Organisational Experiences," *Oslo: Insitute for Social Research* (2013), 10-14; and Gary H. Roseman Jr. and E. Frank Stephenson, "The Effect of Voting Technology on Voter Turnout: Do Computers Scare the Elderly?", *Public Choice* 123, no. 1 (2005): 39-47. New e-voters tend not to be new voters, but instead the technologically savvy portion of the existent traditional voter pool. A study on turnout in Estonia from 2005 (when the law was passed) to 2015 found a small increase in turnout following the introduction of e-voting, but not a causal connection. Mihkel Solvak and Kristjan Vassil, *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years* (Tartu, Estonia: Johan Skytte Institute of Political Studies, 2016), 11-12, 169.

object to e-voting generally, but ruled that the relevant legislation was not specific enough on the duties of the Election Commission, the specifications of the technology to be used, and the protection of the principles of secrecy and publicity. Although there was no evidence of malfeasance, the law left open the possibility of tampering. A CD-ROM with the election data stored on it that could be used to print the data at any point was found insufficient as a paper record. The court noted that electoral principles require public access to the system used and the underlying software, including the source code. Because the e-vote was remote, regulations therefore had to be at least as stringent as regulation of postal voting. Austrian law requires that student elections are held Tuesday through Thursday, and e-voting was available from the preceding Monday through Friday. The court ruled that this also violated the law. The ruling was in 2011, after the terms of the representatives elected in the 2008 election had expired, so no election was annulled.

Ensuring Cybersecurity in Elections

While not enshrined in case law, punitive measures imposed on the EMB in the Philippines in 2016 are instructive in terms of the EMB's responsibility for cybersecurity in elections. In March 2016, the Philippines Commission on Elections (COMELEC) was hacked by a group called Anonymous Philippines. The hackers took over COMELEC's website, which was temporarily shut down in the aftermath, and released extensive voter information, including fingerprints. Following the attack, the National Privacy Commission recommended criminal charges against COMELEC Chairperson Andres Bautista for negligence. In its decision of December 28, 2016, the commission stated that "the willful and intentional disregard of his duties as head of agency, which he should know or ought to know, is tantamount to gross negligence. The lack of a clear data governance policy, particularly in collecting and further processing of personal data, unnecessarily exposed personal and sensitive information of millions of Filipinos to unlawful access."[76] The commission did not find Bautista guilty of helping with the attack, but did establish a precedent of holding EMBs and their leadership accountable for information security failures and data breaches in elections. The commission ordered COMELEC to implement new security measures, conduct a privacy assessment, appoint a Data Protection Officer, and establish a Privacy Management Program and a Breach Management Program. Less than a month later, a computer was stolen from the Office of the Election Officer (OEO) in Lanao Del Sur, which the National Privacy Commission noted was "COMELEC's second large-scale data breach in a span of less than a year."[77] The computer contained biometric records of registered voters. Chairperson Bautista was impeached in October 2017 and resigned that month. Bautista was accused of mishandling the data hack, receiving payment from the company whose voting machines were used in the 2016 elections, and failing to disclose his assets. As of the time of writing, a Senate inquiry is ongoing. The Philippines case is a compelling example of potential institutional and personal liability for EMBs and election officials with

[76] National Privacy Commission, "Privacy Commission recommends criminal prosecution of Bautista over "Comeleak," January 5, 2017, https://www.privacy.gov.ph/2017/01/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/.

[77] National Privacy Commission, "NPC starts probe into COMELEC's 2nd large scale data breach; issues compliance order," February 20, 2017, https://www.privacy.gov.ph/2017/02/npc-starts-probe-comelecs-2nd-large-scale-data-breach-issues-compliance-order/.

respect to cybersecurity in elections, and the role that privacy commissions may play with respect to oversight of personal data in elections.

III. Types of Exposure that Can Impact Cybersecurity

Drawing on the themes, trends, and approaches that emerged from the literature review, we have identified five different types of exposure an EMB must consider in its use of data management technology platforms. These different types or "dimensions" of exposure have informed the development of IFES' HEAT process, which is outlined in the next section of this paper.

a) Technology Exposure

Election management systems for various parts of the electoral process are becoming increasingly automated or digitalized,[78] including voter registration, voter identification and authentication on Election Day through electronic voter lists (e-poll books), party and candidate registration, and tabulation of election results, among others. In IFES' experience, most countries running elections today have automated and digitalized at least one of these processes, most commonly the tabulation of results. Unfortunately, there are myriad ways a piece of technology or an entire system can be misconfigured or compromised, deliberately or otherwise. While there are various applicable international principles and guidelines, as discussed above, there are usually no country-specific standards for employing automated or digitalized systems in elections, with some exceptions.[79]

The danger of cyberattacks on EMBs has become ubiquitous, and the level of sophistication of such attacks varies. Perpetrators range from under-resourced and often young individuals, who want to commit vandalism, gain notoriety, or make a political statement by defacing an EMB's website, to Advanced Persistent Threat (APT) groups, usually cyber offensive groups supported and financed by states that want to inflict damage during elections or as part of hybrid warfare. Attacks can therefore range from simple hacks using existing penetration testing tools (for example, Kali Linux)[80] to advanced exploitation of a hardware or software vulnerability that might not even have been documented before the attack (known as zero-day exploits).[81]

[78] Automation is converting to automatic operation, without the need for human assistance, while digitalization is converting data into a digital form that can be processed by a computer.

[79] In the U.S., the EAC has produced Voluntary Voting System Guidelines, which were last updated in 2015 but are continuously developed. *See* "Voluntary Voting System Guidelines," Voting Equipment, U.S. EAC, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/. These are a set of specifications for basic functionality, accessibility and security capabilities of voting as well as election management systems. While these guidelines are non-obligatory at the federal level, except those obligations stemming from the Help America Vote Act of 2002, a number of U.S. jurisdictions have adopted them as obligatory or introduced parts of the standards in their state legislation. *See* "Help America Vote Act," About U.S. EAC, U.S. EAC, https://www.eac.gov/about/help-america-vote-act/.

[80] Kali Linux, https://www.kali.org/.

[81] There are a number of possible attack vectors from external locations, such as SQL injections, DNS hijacking, cross-site scripting, rootkits, etc.

Wide interconnectivity also creates possibilities for novel attack vectors. In 2016, for example, a botnet[82] (Mirai Botnet) was discovered in a small jewelry store, and was eventually found to have compromised 25,000 CCTV cameras globally (Mirai Botnet), raising a concern that certain types of devices can be compromised even during their production.[83] The so-called Internet-of-Things (IoT) – which is basically the concept of connecting any device with an on and off switch to the internet or to other devices – allows for a constant and substantial increase in the number of internet-facing devices that may be ripe for exploitation by malicious actors.[84] Internet-facing systems with limited capacity that depend on their own organization's resources to function and be maintained can also be open to distributed denial-of-service (DDoS) attacks. In Estonia in 2007, a DDoS attack nearly shut down internet infrastructure in the country, while in Kyrgyzstan in 2009, hackers effectively took the country offline after a ten-day DDoS cyber assault, eliminating 80 percent of the country's online capacity. DDoS attacks flood the system with numerous requests from many different locations. Due to limited resources, EMBs typically do not have the capacity to withstand persistent, powerful DDoS attacks without some external assistance. DDoS attacks will always be a threat, since they are inherent to the free design of the system. For example, election results reporting can be targeted by a DDoS attack during election night, when the interest of election stakeholders peaks in a very short period of time and the impact of denied service will therefore be significant.

Beyond deliberate attacks, election technologies are also vulnerable to misconfiguration, accidental misuse, deterioration (especially in transfer or storage), and various types of hardware and software failure. For example, in the 2013 electoral process in Kenya, a significant number of voter identification kits suffered battery failures. Election technology may also require back-up satellite coverage in the event of cellphone or internet failure. It is, therefore, paramount that there are contingency procedures in place, sometimes requiring reverting back to pen and paper.

b) Human Exposure

The need to protect systems from cyberattacks might be obvious, but it is still off the radar of many organizations' decision-makers. A 2018 research survey by PricewaterhouseCoopers (PwC) posited that almost half of company executives lack an overall information security strategy and that many

[82] A botnet is a string of connected computers coordinated together to perform a task. See "What is a botnet?" Malware, US Norton, 2018, https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html.

[83] Daniel Cid, "Large CCTV Botnet Leveraged in DDoS Attacks," *Sucuriblog*, June 27, 2016, https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html.

[84] For example, this number increased by a third from 2016 to 2017. Researchers suggest that future cyberattacks are imminent and that IoT devices must have patchable firmware. Derek Hawkins, "The Cybersecurity 202: Here's what security researchers want policymakers to know about the Internet of Things," *The Washington Post,* August 10, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/10/the-cybersecurity-202-here-s-what-security-researchers-want-policymakers-to-know-about-the-internet-of-things/5b6c6ec91b326b020795603d.

executives are still beginners in data-use governance.[85] This is typically a problem of vertical disconnect between decision-makers and IT specialists, and EMBs are no exception. Most EMBs lack a dedicated cybersecurity officer. Election commission members often do not understand or appreciate the cybersecurity dangers associated with their decisions. When they do, they may resort to hoping their systems are obscure, irrelevant, or beyond the reach of hackers. Given how important elections are, this is a systemic fallacy with dire consequences.

The failure of decision-makers in EMBs to understand the importance of cyber protection usually goes hand in hand with a lack of basic cybersecurity practices (commonly referred to as cyber hygiene) used by staff on computers connected to sensitive networks. In some situations, this even extends to IT staff.[86] Inadequate cyber hygiene may or may not be compounded by a lack of understanding of the social engineering aspects of a cyberattack. For example, it can require training to understand the dangers of impersonation during unsolicited communication, as well as the difference between requested and unsolicited conversation over the phone or other communication channels, such as emails or chat on social networks.

Three of the major ways in which EMBs are vulnerable to human exposure are phishing attacks, watering hole attacks, and insider attacks. Phishing attacks are cyberattacks through impersonation or other fraudulent action, performed to gain access to systems or to some piece of information, such as passwords. This method of attack was used by Russia in targeting the presidential campaign of Hillary Clinton in 2016.[87] A phishing attack aimed at specific personnel, such as the most vulnerable staffer who knows the least about security or exhibits the most lax behavior, is referred to as spear-phishing. Most adversaries target the weakest link to make such attacks affordable, so high-tech responses aren’t necessarily the right answer.

If an attack is also aimed at high-level executives or decision-makers, it is commonly known as whaling. One of the most common attack vectors in spear-phishing is fraudulent emails (also referred to as spoofing) or clone-phishing (where a legitimate and previously delivered email is cloned and malware inserted).[88] In case of high-level attacks by advanced hacker organizations, emails are crafted to be virtually indistinguishable from legitimate intra-institutional emails and may contain links with malware. Once the victim clicks on the link, the damage may already be done, and it may take substantial effort and training to remove the malware. Watering hole attacks are where a hacker or hacking group guesses or observes which websites an organization’s employees often uses and infects one or more of them with malware in order to ultimately infect the organization’s network.

[85] Christopher Castelli, *Revitalizing privacy and trust in a data-driven world: Key findings from The Global State of Information Security® Survey 2018,* PwC, https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf.

[86] For example, IT specialists may sometimes avoid installing anti-virus software on their workstations only to avoid computation overhead, especially if they have to operate on outdated hardware.

[87] Intelligence Community Assessment, “Assessing Russian Activities and Intentions in Recent US Elections,” January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[88] Computero, “How Not to Go Phishing,” May 16, 2014, https://computerobz.wordpress.com/tag/clone-phishing/.

Insider attacks represent yet another attack vector that can be devastating. If an adversary has physical proximity to an election system, it may be easier to procure or install a malevolent player inside an EMB, which can inflict serious damage to election systems. An insider attack may also come from an individual acting destructively to achieve some political goal. Insider attacks may come from weak physical security of systems, inadequate vetting of contractors, or even poor hiring and employment practices. A related problem is the limited pool of experienced IT experts willing to start or continue working for EMBs. EMBs typically pay salaries comparable to the rest of the public sector, while good IT experts can earn much more in the private sector. While this may be a problem for any type of expert working with an EMB, where the responsibility is enormous and wages limited, it is even more so with IT. Incentives must be considered when evaluating human exposure. A related challenge is the requirement for even greater openness and transparency to EMB systems and platforms for stakeholders such as observers and party agents, which as seen in Kenya in 2017 may even be ordered by the courts. This presents even greater entry points for human mistakes or interference, and argues for a careful security credentialing process and oversight and monitoring of stakeholder access.

c) Political Exposure

There is no end to the ways in which an EMB can be exposed politically, sometimes by their own action or inaction, especially in developing democracies where checks and balances may not be in place. It takes significant time and effort to build trust in elections and the institution running an election but takes very little to lose that trust. For example, if corruption is alleged during a procurement process for new election technology, whether proven or not, this can significantly impact public perceptions of the EMB. Types of political exposure include political influence on EMBs to adopt certain types of election technology, improper influence over election technology procurement processes, and allegations of improper technology use that is designed to cast doubt on the institution, process, or outcome.

Procurement of election technology can be particularly fraught, especially as technology vendors access senior political figures promising an easy fix to integrity issues, or as citizens look to technology for a solution for perceived failures in the electoral process. This can leave an EMB exposed when they face pressure to adopt a certain technology or are influenced in the procurement process to use a sole-source procurement or select a preferred provider.

A particular concern in the procurement process is commonly termed “vendor-lock.” As the ACE Electoral Knowledge Network notes, “[w]here technology is proprietary to a vendor, where data formats are not open, or when an EMB relies heavily on a vendor for its electoral operations, it risks being locked into a particular vendor…[a]ny such tie to one particular vendor should be avoided to make sure the EMB remains in control of the systems it uses and the costs incurred.”[89] Beyond being locked into one vendor, there can be flow-on risks and costs in the vendor relationship that can leave an EMB exposed. For example, in The Gambia, in response to criticism following the 2011 election cycle, the Independent

[89] ACE: The Electoral Knowledge Network, “Election Technology Vendors,” https://aceproject.org/ace-en/topics/em/emia/emia03.

Election Commission (IEC) contracted an international vendor to centralize and digitize the voter register into a single national database that promised biometric de-duplication through fingerprint matching. The 2011 presidential election was held on the basis of the new centralized register. However, given the specific contractual arrangements and proprietary technology in place with the vendor, the IEC remains unable to independently perform data queries, updates, or de-duplication. In advance of the 2016 presidential election, the IEC paid the vendor nearly half the cost of the entire election for its assistance in undertaking The Gambia's first and only voter registration update since 2011.[90] At a cost of 7.9 Euro per registered voter (comparatively extremely costly), the IEC recorded 89,649 new entries, and made no deletions or address changes.[91] It remains unclear whether any de-duplication, the predominant reason to implement biometric technology, was ever performed.[92] This also undermines attempts by the EMB to ensure data security on its servers and safeguard the database from leaving its premises.

Relying on an external vendor can also result in political exposure, opening up the process to accusations of foreign interference. The Democratic Republic of Congo (DRC) is currently facing controversy over its procurement of EVMs from a South Korean company, Miru Systems. South Korea's National Election Commission has come out against the decision, saying the machines are ill-suited for the Congolese electoral environment. Opposition in the DRC have objected to the machines too, calling them "cheating machines," a clear case of the use of a foreign vendor lowering trust and providing a pretext for contesting election results. [93] Following the August 2017 presidential election in Kenya, members of Parliament affiliated with the opposition accused the technology vendor, based in France, of providing kickbacks to the EMB and ruling party, while "willfully allowing" unauthorized access to its systems and therefore abetting rigging.[94] At the same time, concerns may be raised around privacy of citizen data, including biometric information – especially in countries that are collecting voter data and do not have data protection laws in place, or where data is kept on servers outside the country, raising the risk that such data could be exploited.

There are a number of countries in which the central election authority is a de facto extension of the government, regardless of the EMB's formal status as an independent commission. In countries where political parties appoint election commission members, the ruling party may have a dominant position. This can lead to data security breaches, such as breaches of voter registration data stored in the central election office. If an IT staffer receives an order from a politicized EMB commissioner to copy the entire voter register onto a USB flash drive, he or she may do it without questioning, fearing repercussion. Such actions may go unrecorded and ultimately unsanctioned. The HEAT process outlined below would

[90] The vendor provided new hardware (server and 70 laptops) and the assistance of two external experts.
[91] For additional information, please see: UNDP and IFES, *Getting to the CORE, A Global Survey on the Cost of Registration and Elections*, 2005, http://aceproject.org/ero-en/misc/undp-ifes-getting-to-the-core-a-global-survey-on/view.
[92] IFES Electoral Integrity Assessment, The Gambia, 2017.
[93] "South Korea election panel attacks DR Congo voting system," *The Sun Daily,* April 10, 2018, http://www.thesundaily.my/news/2018/04/10/s-korea-election-panel-attacks-dr-congo-voting-system.
[94] Patrick Lang'at and Silas Apollo, "Nasa: We don't want Al Ghurair and Morpho in poll," *Daily Nation,* September 18, 2017, https://www.nation.co.ke/news/politics/Nasa-MPs-raise-bribery-claim-in-Kiems-kits-tender/1064-4101748-ev0kq3z/index.html.

game out these types of risks and make sure this is part of the information and communications technology (ICT) system protocol so that supervisors automatically get warnings should these types of cases emerge. IT personnel may also require particular protection from political influence or interference, compounded by the fact that qualified IT personnel may be difficult to recruit and retain, as discussed above.

Failures of trust, such as perceived inflation or deflation of voter lists, persist around the world. Apart from procedural aspects plaguing the accuracy of voter lists, which are categorized herein as *procedural exposure*, the electorate may perceive that voter data is not held securely. For example, there might be rumors that the government is printing fake ID cards to impersonate voters (these voters may be deceased or residing abroad but still listed on the voter rolls). It is difficult to prove such claims without conducting a comprehensive audit, but the shadow of doubt may very negatively impact the process. Finally, the collection and processing of election returns is now semi- or fully automated for EMBs that use “contained” results management systems. The associated processes may also be burdened by political considerations. For example, given a choice, EMBs would typically err on the side of protecting the perceived integrity of election results rather than providing maximum transparency. They may decide to publish only the summary results and not the full breakdown of results by polling stations. One example of a practice increasing the transparency of and trust in a system, without compromising security, is in South Korea. Voters mark physical ballots, which are sealed and transported to a constituency counting center. There, in front of political party observers, ballots are scanned and counted using optical scan voting systems. Teams feed ballots into the machines, which then emit stacks of 100 votes for the same party. These stacks are run through the machine again to be counted, and observers are present for both processes.[95]

d) Legal Exposure

It is important for primary election legislation to contain provisions enshrining principles governing the creation, use, processing, and publication of data in elections, without being so prescriptive or opaque that they create challenges in implementation. Without a clear and implementable legal framework, the EMB may face legal exposure either in terms of potential lawsuits against different parts of the electoral process, or with respect to legal restrictions that make the procurement or use of election technology difficult in practice. For example, the law may be so prescriptive that it requires an EMB to procure and deploy specific technology platforms within unrealistic deadlines, and this may set the EMB up to fail well before the election is initiated. Or, as in the case of Kenya, the EMB may be required by law to submit regulations governing election technology for parliamentary approval, which opens these rules up to modification by political actors who do not have any practical technical knowledge.[96]

[95] Tim Meisburger, “Korean Elections: A Model of Best Practice,” The Asia Foundation, 2016, https://asiafoundation.org/2016/04/20/korean-elections-a-model-of-best-practice/.

[96] Section 44 (5) and section 109 of the Kenya Elections Act, 2011.

There are also broader principles that should be enshrined in law to avoid political exposure for the EMB in terms of cybersecurity. For example, if the election law does not clearly establish the independence of the central EMB and grant the EMB full control over their secretariat, the government, or certain quarters within it, may be tempted to install its own personnel in key IT positions. Since the issue of cybersecurity is often considered a matter of national security, there may be situations where the articles governing national security and EMB independence contradict each other. In terms of accountability, laws often establish shared responsibility for managing information assets, most importantly for voter registration data. In countries with passive registration systems, EMBs often depend on local and state authorities for voters' citizenship and residency information. Even though the central election commission may be responsible for the accuracy of voter lists, it cannot fully control the process. The shared responsibility must be managed properly in the law or run the risk that no one is held accountable.

In terms of data privacy, the authorities need to make sure that election legislation is harmonized with data protection legislation or includes articles about the protection of private citizen information, drawing on international principles. Similarly, important transparency measures should be enshrined in law, but without being overly prescriptive, and in a way that is supported by time and resources (for example, adequate provision in the EMB budget). At the time of writing, the opposition party in Zimbabwe has filed a petition in the Supreme Court seeking to nullify the election result, with one of the grounds being that the EMB did not release the entire final voter roll on a USB, as the EMB decided not to include photographs and biometric fingerprints. An EMB might consider their primary role to be managing elections without irregularities, even at the expense of transparency. As a result, they may forbid observers from coming too close to data-entry personnel who tabulate election results, whether for the sake of physical security or a calmer working environment. Even when an EMB wishes to be more transparent, they may value control over transparency to be safe. If the law establishes that transparency of information is one of an EMB's core functions, the EMB will be required to strike a balance and allow closer access to observers.

There are significant associated costs in ensuring transparency, especially in terms of information management. For example, if an EMB wants to be transparent about gender-disaggregated polling data, they need to be able to count and record this information at the polling station level and to publish the relevant data. This may be more difficult than it seems: some polling officials may fail to record gender information, or there may be technical challenges in the disaggregation process. An EMB that is legally required to disseminate this information must have the resources to properly design data-collection methodologies, train staff, securely store data, and publish information in an accessible format. Pakistan has recently included the requirement for gender-disaggregated data in its new election rules.[97]

[97] Democracy Reporting International, "From Law to Action: Election Reforms in Pakistan," 2018, https://democracy-reporting.org/from-law-to-action-election-reforms-in-pakistan/.

Finally, with respect to legal redress for election irregularities, because the gathering of evidence in annulment cases, and election cases generally, can be extremely difficult, the role of the election commission can be of critical importance.[98] In some cases, the EMB will be the only party in a position to investigate irregularities.[99] In other cases, the EMB may be best able to determine the impact of the irregularity. Unfortunately, modern data management systems may not produce evidence traditionally accepted in courts or may produce evidence that requires specialized understanding by an adjudicator. For example, there may be digital data logs showing that an event occurred, but adjudicators would need to understand how such files could be easily falsified without leaving a trail, or how they can be signed digitally to clearly establish authenticity. Laws or rules on civil procedure and evidence may not be appropriately drafted to account for specific evidential needs or timelines for election cases, and this may ultimately impact the right to redress and the provision of electoral justice.

e) Procedural Exposure

Every EMB has a plan for running elections, but if election commissioners do not understand how modern data management systems work, there may be a procedural gap. The proper operation of computerized election systems within an EMB should be formalized through regulations and procedures prescribing a certain level of detail. The main principles related to functionality, operability, and security should all be laid down explicitly. Otherwise, critical issues may occur during the run-up to the election. For example, the design of systems may turn out to be a patchwork of partial plans and there may be gaps or confusion over who does what and when.

Formalizing election operations into regulations or bylaws increases transparency, as these provisions are made available to election stakeholders and the public. An EMB that formalizes how they deal with personal voter data can later be held accountable if they do not follow their own rules. However, EMBs can be legalistic or risk-averse and may refrain from interpolating the election legislation with more detailed procedures for fear of being accused of straying outside their remits. Instead, EMBs in many cases go to the other extreme and simply repeat language of the primary legislation. In some cases, the government or legislature must approve administrative regulations, and this may impact the quality of rules adopted. Or, detailed procedures may be developed internally by the EMB but not formalized or widely published. Such internal procedures are neither transparent nor externally tested, and are often not under the full control of the commission as the collective and collegial body.

[98] For a discussion of legal approaches to election annulments, see IFES' forthcoming paper: "Annulling Election Results: How Many Irregularities Are Too Many?" http://www.ifes.org/news/annulling-election-results-how-many-irregularities-are-too-many.

[99] To play this role, the EMB must be equipped to properly conduct election investigations within tight timelines and to handle evidence appropriately to ensure it is admissible. General Comment 31 to the ICCPR: "Administrative mechanisms are particularly required to give effect to the general obligation to investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies." IFES has outlined key principles for election investigations in a forthcoming publication *Standards, Techniques and Resources for Investigating Disputes in Elections* (STRIDE).

EMBs also typically lack comprehensive cybersecurity strategies. If an EMB does not lay down their system design in detail, they will not be fully aware of its potential vulnerabilities and the security assumptions they make. If they do not evaluate potential threats, both internal and external, they will not be able to prepare themselves for cyberattacks. And if they do not collaborate with external institutions, such as consulting their country's CERT organization and data security standards, they may fail to employ best practices in cybersecurity. After introducing EVMs, the Indian Election Commission claimed their machines were invulnerable to attacks. When a group of ICT experts published a paper in 2010 arguing that the EVMs were in fact susceptible to cyberattacks, police arrested one of the writers and researchers, interrogating him over how he had accessed one of the machines (he was released soon after).[100] In 2013, the Supreme Court of India validated the experts and ordered the phasing-in of VVPATs for the machines. VVPATs are now used in Indian elections as a back-up security measure. EMBs must be aware of the security flaws in their technologies and plan accordingly.

IV. Holistic Exposure and Adaptation Testing (HEAT) Process

a) What Is a HEAT Process and What Is It Not?

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

The HEAT process is *not* intended to provide certification of any systems. Technology certification is a specific process of evaluating voting hardware and software to ensure they provide all the basic functionality, accessibility, and security capabilities required. There are various challenges associated with pure "certification" processes in practice, in which only the hardware or software is considered in isolation from the wider electoral environment. In 2010, the Philippines COMELEC sought a vendor to certify their EVMs. It was clear from the outset that any company contracted for certification would identify several potential security flaws and would make recommendations to absolve themselves if anything went wrong. The company ultimately chosen, SysTest Labs, noted that the EVMs were appropriate for their intended use, but only under certain conditions. SysTest Labs recommended adequate safeguards and procedures, including a "statistically significant random manual audit" and a disaster recovery plan. They recognized risks to using the machines, and their recommended procedures were meant to detect potential flaws and to scrap the automation if necessary, even mid-election. In

[100] Matt Ford, "Indian Democracy Runs on Briefcase-Sized Voting Machines," *The Atlantic,* April 15, 2014, https://www.theatlantic.com/international/archive/2014/04/indian-democracy-runs-on-briefcase-sized-voting-machines/360554/.

Kenya, the IEBC started the process of finding a certification and testing company but discovered that no company was willing to certify the technology without access to manual processes, chain of custody, source code review, procurement transparency, and other similar information. Certification was ultimately not pursued.

There are various other types of testing processes that can also examine elements of election technology development or use. *Logic and Accuracy (L&A)* testing is the process by which voting equipment is configured, tested, and certified for accuracy prior to an election. Each component is tested to verify that it is fully functional and free from mechanical problems and that each voting unit contains the appropriate ballot styles for its designated polling place. *Penetration testing (pen tests)* consists of a variety of tools used to identify technology vulnerabilities, including *port scanning*, *vulnerability scanning* (software and firmware), *packet sniffing*, and review of log files. A *risk-limiting post-election audit* checks a random sample of voted ballots, or voter-verifiable records, in search of strong evidence that the reported election outcome was correct.[101] If the reported outcome is incorrect, then the audit may lead to a full hand re-count that reveals the correct election outcome. By design, once the audit finds strong evidence that the reported outcome was correct, it can stop. Thus, the audit adapts to the facts of a particular election. Following the 2016 elections in the U.S., and the designation of election systems as "critical infrastructure," the U.S. Department of Homeland Security designed a variety of testing and review processes (outlined in the text box at right) that it has offered to states. However, these testing processes are focused primarily on the technology system itself, and are subject to lengthy delays that raise challenges for states seeking to implement changes ahead of elections.[102]

Types of Testing and Review Provided by the U.S. Department of Homeland Security

Risk and vulnerability testing: *A multi-week probing of the entire system required to run an election*

Cyber-infrastructure survey: *An expert-led assessment accomplished through informal interviews*.

Cyber-resilience review: *Helping election officials conduct their own self-assessments*.

Cyber-hygiene scans: *Probing election systems remotely and reporting vulnerabilities*.

IFES aims to incorporate elements of existing testing processes within a straightforward, holistic testing process that can help an EMB correct vulnerabilities in the system that could lead to known or unknown manipulation of election data, system failure, or future legal challenges. The HEAT process will not be a mechanism to approve or reject the decision to use a particular technology or a particular vendor, although it can inform effective vendor relationships and cybertechnology supply chain threats, as well as the interaction between different technology platforms that might be used in different parts of the electoral process. A HEAT process can also help an EMB prepare for the resources and processes they

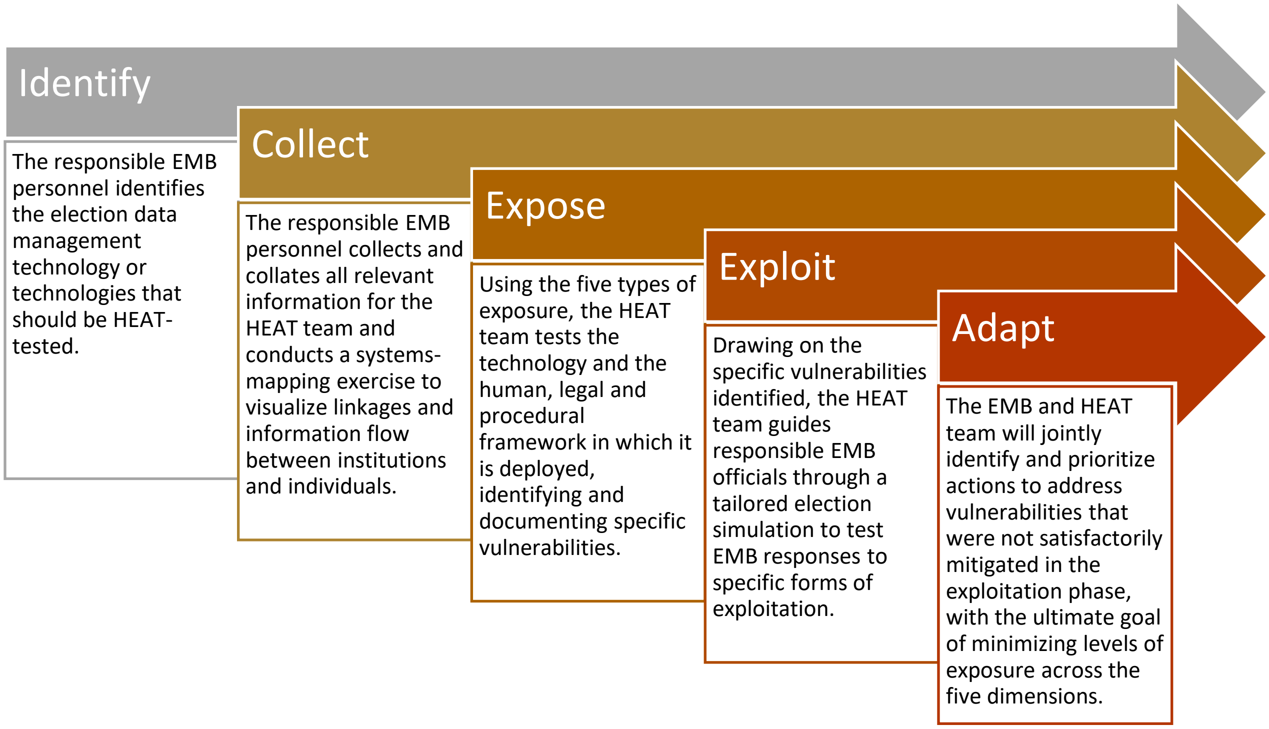
[101] Mark Lindeman and Philip B. Stark "A Gentle Introduction to Risk-Limiting Audits," *IEEE Security and Privacy, Special Issue on Electronic Voting, 2012,* https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[102] Tim Starks, "The latest 2018 election-hacking threat: 9-month wait for government help," *Politico,* December 29, 2017, https://www.politico.com/story/2017/12/29/2018-election-hacking-threat-government-help-231512?cid=apn.

will need to have in place in the event a security breach or system failure occurs, or in case the system is challenged in court. This is particularly important with respect to the type of evidence required and admissible with respect to election technology, and to establish a chain of evidence that can be used in future legal challenges. ICT officials need to work closely with legal officials within an EMB to address this vulnerability.

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

b) Outlining the HEAT Process



Identify

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

Collect

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

Expose

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

Exploit

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

Adapt

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

Identify

The HEAT process is designed to be EMB-led and provide a capacity-building element for the EMB, as opposed to an external assessment. As such, the first step of the HEAT process is undertaken by the

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

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

Collect

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

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

System mapping can shine a light on otherwise hard-to-identify incentive structures, interactive effects and leverage points for identifying and addressing vulnerabilities in the electoral process. Without a consideration of the system design (a system map) and the underlying cybersecurity assumption, it is very difficult to recognize the existence of all the specific vulnerabilities. A system map is a visual depiction of the components of a system at a point in time, while an actor map is a type of system map that focuses on relationships and interconnections between various actors involved in a system. These maps help show how the parts of and people within a system are connected, identify weak connections or gaps, bring out ideas for intervention points in the system, and help identify ways of determining whether these changes have occurred. The HEAT team will provide instructions and templates, or can directly guide the EMB through this process. The resulting map will form part of the HEAT team's exposure process in step three.

Expose

Step three requires the HEAT team to collectively analyze the relevant EMB materials and systems map and expose vulnerabilities within the five different types of exposure – technological, human, political, legal and procedural. Because the process looks holistically at these five different types of exposure, the HEAT team should generally consist of a technology expert, legal expert, and election operations expert. Step one of the HEAT process should feed into the identification of the HEAT team, in terms of the specific technology or technologies being tested. The core question will be: who is qualified to help test and assess the election technology and the framework or context in which it is deployed? Once identified, during this part of the process the HEAT team will identify and record vulnerabilities that the EMB faces in using the specific technology being tested, categorized under the five types of exposure, and will list preliminary options for mitigating or managing vulnerabilities.[103] In addition, the HEAT team should look at certain external elements that can significantly impact the election process, especially in terms of possible negative influence or disinformation campaigns against the EMB or other election stakeholders, and will examine existing EMB communication strategies.

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

Exploit

Drawing on the specific vulnerabilities identified during steps two and three, the HEAT team will guide responsible EMB officials through a tailored election simulation tabletop exercise (TTX) to test EMB responses to specific forms of exploitation. A TTX is a training simulation that mirrors real-world conditions, uses an accelerated timeline to increase pressure, gives everyone a role with corresponding responsibilities, and enables participants to absorb information, make decisions, and execute plans. It is similar to the "red-teaming" process used by the U.S. Department of Defense to "challenge emerging operational concepts in order to discover weaknesses before real adversaries do."[104] The HEAT team will draw on the vulnerabilities identified in step three of the HEAT process and test participant responses as these vulnerabilities emerge or are exploited in a simulated environment. This step has two purposes – testing existing capacity and responses of EMB officials and serving as a more impactful learning exercise for officials who will be responsible for making necessary changes to reduce EMB cybersecurity exposure. Lower-level commissions require substantial training related to the election process, in general, and cybersecurity is no exception. The TTX can help reveal and emphasize for EMB officials the exact training needs required for different staff in the EMB, for example around cyber hygiene and spear-phishing.

Adapt

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

In terms of technology exposure, some of the essential tools that EMBs might consider using to avoid system crashes are carefully designing systems, testing, set-up, configuration, piloting, audits and contingency planning. EMBs should have back-up plans for new systems, including the possibility to revert to old systems in the event of a crisis. For example, if seat allocation is relatively complex, the EMB that bears responsibility may decide not to rely exclusively on software being used for the first time, even if that software has been tested.[105] EMBs should have advanced network-monitoring capabilities to determine with some level of certainty the nature of events that occur in its systems. Having a strategy in place would allow EMBs to react quickly, apply contingency plans, or restore from backups.

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

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

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

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

The EMB may have certain cybersecurity practices in place, but those might be scattered in multiple documents, informal files kept by IT specialists, or not even recorded in written form, but only employed in practice. The HEAT team should encourage the EMB to consolidate and lay down all their security practices and assumption in one place; in this way, they will be more accessible, transparent to the EMB, and possible to be challenged (for example, if the system does not place any constraints on the size and structure of passwords, this can be highly problematic). This, if formalized, can become the EMB's cybersecurity strategy. The establishment of such a strategy will increase the EMB's resilience against cyberattacks.

Ultimately, the goals of the HEAT process are to holistically test specific election technology systems for vulnerabilities, to directly involve relevant EMB officials in the process and ensure it can be an exercise in capacity development, and to identify adaptations that the EMB can lead or influence to reduce cybersecurity exposure levels.

V. Conclusions

As identified at the outset of this paper, EMBs increasingly rely on complex technology in electoral processes. This has created new security challenges related to protection and safekeeping of election data in digital form and related computerized systems. Most countries now automate and digitalize at least part of their elections, from the use of e-voting to electronic voter databases. The issues around cybersecurity in elections are therefore increasingly universal and are becoming more complex.

Adversaries, whether individual or state, find new ways to disrupt election processes, and new technologies require staff to be trained on how to use them and how to protect data. Even when cyber defense is perceived as currently adequate, rapid technological innovation means that EMBs should focus on potential vulnerabilities in the *next* election, not on vulnerabilities detected in the *last* one.

Potential vulnerabilities in electoral cybersecurity are not limited to technology, but are also human, political, procedural, and legal. In this paper, IFES has sought to identify potential exposures and a set of cross-cutting processes to address security threats holistically. Part of the ambition of this paper is to bring lessons from the empirical literature together with the understanding of the variegated nature of cybersecurity threats in elections. While no method or technology is infallible, the HEAT process aims to secure electoral processes as much as possible against unanticipated threats, illicit incursions, system failures, human error, perception issues, or unfounded or excessive legal challenges.

To avoid potential legal exposure similar to the 2008 Austrian student elections court challenge, EMBs and their governments should work together to draft clear election technology legislation and regulations. The NIST framework is a comprehensive tool to use as a starting point to reduce technological exposure, and resources such as the UNDP/European Commission's *Procurement Aspects of Introducing ICTs Solutions in Electoral Processes* can help EMBs develop technology more securely and effectively to avoid political exposure that can lead to a reduction in public trust in the EMB and the government. Signing and following the principles in the Open Government Declaration can also signal a clear intent of transparency, and the participation of observers can help legitimize an election in the public's eyes, with sound observation methodologies that account for election technology platforms and that differ in many ways from traditional observation of paper-based elections. In the future, there would be value in various international technical assistance providers coming to consensus on IT governance standards for elections management, along the lines of the Declaration of Principles for International Election Observation. An alternative approach might be to raise the need for standards in regional or global EMB associations that currently exist.

Transparent and clear strategies build trust, but they also protect EMBs from blind spots and increase accountability. Although they are not election-specific, international standards such as the UN General Assembly Guidelines for the Regulation of Computerized Data Files provide broad data management principles that place responsibility for data on the persons who collect it, helping protect against procedural exposure. The guidelines specifically require that data collectors be responsible for ensuring that the data is accurate, transparently and lawfully collected, properly restricted to avoid discrimination, securely stored, and lawfully disseminated.

Finally, even more fundamental than best practices is acknowledging the need for those practices, an essential part of minimizing human exposure. EMBs that understand cybersecurity's importance will have more secure elections where others – such as COMELEC in the Philippines, whose commissioner was forced to resign before he could be impeached for negligence after a data breach – will expose themselves to threats unnecessarily. Drawing from its experience and expertise, IFES has sought to take a holistic view of cybersecurity in elections to support our EMB partners from actual and perceived technological failures in the electoral process. The HEAT process framework laid out in this paper is guided by international best practices on data management and cybersecurity, as well as transparency, open data and privacy. The process can help EMBs and other stakeholders develop the infrastructure and systems needed to secure the electoral process as technology changes. A thorough HEAT process, as described in this paper, has significant time and cost implications. However, without such a process in place, an EMB may experience an electoral crisis that goes well beyond the time and expenses they would otherwise invest to protect their cybersecurity.

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS

IFES · 30 Years ·

Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org