insider threat mitigation. Insider threat within the context of EMB operations is still poorly understood and thereby even more difficult to detect and/or address. There are, however, managerial, operational, and technical controls that are designed to help mitigate such threats. For example, sensitive IT processes should utilize "two-person" control whereby two people have to sign off and be involved to successfully complete the task. Another administrative (management) control would be the execution of background checks for EMB employees to help screen out candidates that are more likely to pose an insider threat. In terms of technical controls, automated alerting of suspicious activity such as copious printing outside normal business hours can be utilized to help identify possible exfiltration of data by insiders. These types of controls may not be achievable given the resources available to certain EMBs.

IV. EMB RISK MITIGATION ACROSS THE ELECTORAL PROCESS

Election processes are complex and multifaceted, and vary across democratic systems and contexts. The following subsections highlight the technologies and processes involved with various important tasks in elections, with an emphasis on cybersecurity risks, threats, and mitigation strategies. The controls discussed throughout this sub-section are considered good practices that can be replicated and utilized across an EMB's information technology infrastructure and developed further as EMBs mature their cybersecurity risk management practices.

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

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

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

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

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

A. LEGAL AND REGULATORY CONTEXT

1. CONSIDERATIONS FOR INTRODUCING NEW ELECTION TECHNOLOGY

The specific **operational context** for elections must be carefully considered before introducing, procuring, and implementing new election technology. For example, before using new technology for voter registration, it is important to know who registers voters (the EMB, another government agency, or another organization), who collects data on voters, how that information is shared with the EMB (if the EMB does not collect the data), and who owns the data.[146] New technology typically requires additional human capital considerations, such as stronger information technology (IT) skills and experience as many election staff lack the skills to manage new technology without training.[147] In Kosovo in 2010, for example, local staff were found to need two electoral cycles' worth of training before they would have the IT skills and experience necessary to run the relevant technology on their own.[148] This example highlights the security risks around poorly equipped technology users who may be easy targets for malware on individual terminals that are connected to wider systems and networks.

In addition to the operational context, the **structure of the electoral legal framework** may also present a challenge for the introduction of new technology in the electoral process. The relevant legal provisions may reside in three locations: "the constitution, if there is one, the laws relating to elections (or articles in general laws related to elections, such as for example, the criminal code), and the secondary legislation (such as regulations, rules and procedures often passed by EMBs)."[149] In some cases, legislation governing these technologies may be found in areas outside of elections, such as regulations on data protection.[150] Before working within the existing framework of laws and regulations, it is necessary to address "not only the tools needed, but also the systems and processes that must be reengineered in order to shape an effective solution."[151] As noted by the Council of Europe, any changes to the legal and regulatory system should be accompanied by clear, public explanations of why those changes are necessary, which "will reinforce voters' and other stakeholders' trust and confidence."[152]

An appropriate **timeframe** for procurement, implementation, testing, and training is also a decisive factor in determining whether to use a new technology. Timelines for ensuring a smooth transition to new technology will vary by country. EMBs should have a clear plan, from the initial determination of the technology's merits as applied to the electoral process through final implementation. Introducing new technology too quickly can jeopardize public trust and can lead to technical challenges, further eroding

---

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

trust in the process.[153] A fundamental element that is often inadequately factored into planning is the testing process, which should be part of standard operating procedures. Another key factor to consider is whether there will be a process of systems integration, usually between hardware and software, or the wholescale introduction of new hardware and software into an electoral process. Both can produce vulnerabilities, but systems integration can give rise to unique challenges, particularly where a new solution is essentially bolted onto an existing system or platform.

Legal framework and timeframe challenges may compound each other. For instance, many EMBs introduce election technology with little or insufficient adjustment of the legal or regulatory framework for elections or are compelled to introduce technology due to imperatives added to the law. This can cause significant problems in practice; for example, tight procurement timelines to meet legally mandated election dates might result in insufficient time for effective testing and training (or lead to criticism of the EMB for undertaking emergency or sole source procurements). Provisions in the law may also impact timelines for adoption of new technologies. Some regional principles prohibit amending fundamental elements of the legal framework in election years, as in the Council of Europe and Economic Community of West African States (ECOWAS) regions. This results in countries attempting to implement new operational paradigms within existing, outdated legal frameworks. This is problematic, as legal frameworks are crucial for defining the powers of – and imposing duties of care on – EMBs and EDR tribunals around the deployment and use of election technology.

The level of **public trust and confidence** in the electoral process and the EMB specifically must also be taken into account when deciding whether to implement new election technology.[154] If public trust in the electoral process is already low, introduction of a new system may cause public unrest.[155] To build trust, the Council of Europe recommends public debates or consultations that include all voters. These public outreach activities should lead not only to greater trust in the technology itself but to greater trust in the implementers of the new technology. International IDEA's recommendations include releasing the results of pre-implementation testing, auditing the new technology regularly, and developing and publicizing clear policies "that cover all aspects of technology use."[156] In addition to the voting public, political parties should be consulted. Explicit buy-in from all involved political parties regarding technology and technology implementation can mitigate against contestation later in the electoral process - avoiding costly litigation, audits, and recounts.

Specific tools that provide independent ways to test the system, such as audits of technology systems, are also a good means to gain public trust and secure against fraud.[157] Public communication around contingency planning is also fundamental so that changes in procedure – for example, switching to paper ballots in case of a power outage or security breach – are not perceived as suspicious in and of themselves. As highlighted earlier in the academic literature review, an analysis of Texas counties during the 2020 United States elections conducted by Kasongo et al., highlights that improvements to training, resources, and processes, while helpful for ensuring a smoother election process, may not be sufficient to mitigate

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

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

Other mechanisms can be built into the law to help maintain confidence in the results of elections that leverage technology. One example is tabulation audits, which review a set of ballots, interpret voter intent and check that determination against the results produced by the original tabulation process.[159] Risk-limiting audits (RLA), a type of tabulation audit that relies on statistical evidence to confirm the outcome of an election, are increasingly used in the U.S. context to confirm the machine count.[160] As with other audits, changes may be required in the law and procedures to accommodate the RLA. Specifically, IFES has indicated that the laws should:

- Clearly define the purpose and parameters of the risk-limiting audit;
- Specify how contests are selected to be audited;
- Select an appropriate risk limit ("the predetermined maximum probability that the audit will not uncover an incorrect outcome") or delegate authority for its determination;
- Ensure the timeframe for the RLA is compatible with legal deadlines for election counts and results certification, and that the audit is appropriately harmonized with election dispute resolution processes;
- Provide for public accessibility and verifiability of the entire RLA process; and
- Require security and integrity measures, including appropriate ballot accounting procedures.[161]

2. CYBERSECURITY-SPECIFIC LEGAL AND REGULATORY FRAMEWORK CONSIDERATIONS

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

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

---

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

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

If the law and regulatory framework clearly answers these questions, it will provide EMBs and other electoral institutions both notice of and guidance for how they can meet the challenge of adapting to existing cybersecurity risks. While managerial and operational controls used in business and government agency operations are relevant – including privacy, access privilege, and duty of care – they must be clarified for the electoral context. The post-incident response process also needs to be considered, as the electoral context may demand a more transparent investigation than a private company or government agency might otherwise undertake once a cybersecurity incident has been detected and verified. Elections are fundamentally public exercises, and as such, while EMBs can strive to use risk management-based frameworks for cybersecurity, there is much work to do to sufficiently tailor and define specific mechanisms and controls for the electoral context.

Good practice would also dictate that sufficient time be allocated to adapt the legal and regulatory framework prior to technology procurement, so that it sufficiently takes into account powers and duties to ensure cybersecurity and sets out a framework for contingency measures in the event that a successful cyber attack occurs. The Council of Europe *ad hoc* committee on electronic voting notes that "There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, maintaining, observing and auditing e-voting systems. (…) It is recommended that the relevant legislation provides for the supervisory role of the electoral management body over e-

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

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

CYBERSECURITY IN THE PHILIPPINES ELECTION PROCESS

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

While the Commission did not find Bautista guilty of helping with the attack, it ordered COMELEC to implement new security measures, conduct a privacy assessment, appoint a Data Protection Officer, and establish a Privacy Management Program and a Breach Management Program. Less than a month later, after a computer containing biometric records of registered voters was stolen from a regional election office,[167] Chairperson Bautista was impeached and resigned. The Philippines case is a compelling example of potential institutional and personal liability for EMBs and election officials with respect to cybersecurity in elections, and the role that privacy commissions may play in oversight of personal data in elections.

B. PROCUREMENT AND PLANNING

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

Proper security planning and field-testing with the relevant cybersecurity, law enforcement, military, and private security stakeholders is also important throughout all phases of the electoral process. State election laws in the U.S., for example, require election equipment testing and certification by government-accredited agencies, but most countries that acquire election technology lack such a framework.[168]

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

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

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

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

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

and cybersecurity experts are seldom called upon to serve on tender selection committees. Cybersecurity field-testing or penetration-testing is rarely performed prior to bid selection and contracting. In Pakistan, a Senate Committee recently rejected the acquisition of EVMs on grounds that machines could compromise secrecy of the ballot and would need to be introduced gradually to ensure they were secure from tampering and would not enable fraud.[169] Many countries also do not allow independent observation of election technology testing, which detracts from stakeholder confidence in that technology's protection against cyber attack.[170]

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

Mitigation strategies:

- EMBs should **consider cybersecurity an organizational requirement,** rather than an ICT problem.
- EMBs are advised to progressively **integrate cybersecurity good practices**, with regular assessments of their posture and a risk-based approach to adopting new technologies, including **in their strategic and operational planning and budgeting.**
- The various institutions and agencies associated with general election administration and planning processes should **implement risk management and security controls** according to the ISO, NIST, ENISA or other frameworks.
- It is imperative for EMBs to **develop cybersecurity education and awareness training**, and to **test user readiness** with simulations.[171]
- They should also **engage with other agencies** responsible for the cybersecurity of other aspects of these processes that fall outside of the EMB's purview, creating efficient communication and response channels and plans.[172]
- EMBs should **use the concept of least privilege** as part of their operational and technical controls. This helps ensure that only persons who are authorized, and who need access, can access sensitive information. Further controls can be used to implement comprehensive data loss prevention programs; such programs combine managerial, operational and technical controls to

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

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

- In addition, EMBs should **create clear policies that define acceptable use of technologies within the organization** (e.g., requiring all personnel to use an official, institutional email account – the infrastructure of which is under EMB control – for all communications).
- Finally, EMBs should **embrace cybersecurity as a central procurement criterion** and adjust their procurement timelines and procedures accordingly, while also formalizing the cybersecurity requirements that flow down to contractors.

UNDERTAKING PROACTIVE COMMUNICATIONS IN PARALLEL WITH PROCUREMENT

EMBs should not introduce new technology without an extensive communication and awareness campaign to inform stakeholders. **Procurement and operationalization of new technology should automatically trigger consideration of residual cyber risk, and the roll-out should be accompanied by a well-conceived communication plan**. EMB communication should avoid overselling the cyber-resilience of new technology, and instead emphasize the full array of mitigating measures and contingencies the EMB will undertake to assure the electorate and political stakeholders that the integrity of an election can be verified and upheld, even if a successful cyber attack occurs. EMBs might consider publicly communicating any cybersecurity testing it conducts on new technology.

C. BOUNDARY DELIMITATION

Overview and main uses of technology: The boundary delimitation process refers to drawing electoral district boundaries (or constituencies). It also involves determining electoral precincts and polling locations and assigning voters accordingly. Boundary delimitation typically takes place in the pre-electoral and post-electoral phases.[174] Technology has been increasingly integrated into these processes, replacing mostly cumbersome manual systems that precisely map locations and distribute voters. Technology, when part of a transparent and impartial process, can contribute to processes that distribute voters equitably, that maintain standards of vote weight and ensures the representativeness and non-discrimination nature of electoral districts. [175] This same technology, when used to manipulate electoral districts and boundaries, can be a very effective tool in efforts to gerrymander election districts and manipulate electoral outcomes.

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

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

Mitigation strategies:

- **When systems are connected to outside entities, EMBs should create formal agreements** such as "service level agreements" (SLAs) and memoranda of understanding (MoU) **to define the relationship and responsibilities of each party involved**. In terms of security controls, these agreements should specify cybersecurity requirements and post-incident standard operating procedures to help distinguish responsibilities in case of breach. For example, if an EMB's systems are infiltrated due to connection with a census bureau, does the EMB have the right to inspect the bureau's systems during the investigation?
- In addition, **data exchange should make use of integrity checks to ensure the data received is unaltered from the data transmitted**. In some contexts where the agencies providing data cannot guarantee their integrity, physical transfer (via a USB device) to an air-gapped[176] rather than electronic transfer to a connected database can be advisable.
- **Technical controls**, such as utilizing automated logging and audit solutions where possible, **should be implemented along with data encryption both at rest and during transmission.**

D. VOTER REGISTRATION

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

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

The need to eliminate duplicate voter registrations has made it essential for EMBs to digitize the voter registration process, and today nearly all voter registries in the world are hosted within electronic databases. Most countries operate nationwide voter databases, making them critical infrastructure that could be targeted by cyber attacks.[177]

Several attacks against the confidentiality, integrity, inclusivity and availability of voter lists before and during elections have demonstrated the potential for disruption and damage. Some of the largest data breaches recorded worldwide have been voter list databases, severely impacting the credibility of EMBs.[178]

---

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

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

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

In the U.S., many states register voters by party, making U.S. voter databases especially attractive targets, as a successful compromise can be used to exacerbate partisan cleavages and direct information campaigns based on party affiliation. In addition to allowing online verification of voter registration, many U.S. states have begun to allow online voter registration, and most states have also begun allowing absentee ballot applications online.

Risk discussion: Identifiable risks include breaches or misconfiguration of online cloud storage housing voter registration databases, leading to the exfiltration of sensitive data. Malign actors could potentially target registration databases to place fake records or delete important information as well.[179] Because offline voter registration collection processes are still fairly common in most parts of the world, particularly when collecting biometric data that requires more storage capabilities, laptops or portable media are often used to locally store and transport voter information, making this equipment an attractive commodity if physically stolen. EMBs should consider the cybersecurity risks associated with the integrity of voter registration (both traditional and biometric), including remote access to databases published online, unprotected data transmission from field-deployed voter registration equipment to a central database, and integrity issues related to equipment compromise in the supply chain prior to delivery.

The leak of personal identifiable data is an increasing concern, both due to more mature legal frameworks protecting citizens as well as the advanced capabilities of criminal groups to use stolen data for identity theft. The risk of harm to citizens increases according to the amount of voter registration data collected – more detailed data can mean greater utility to identity thieves. Breaches can also undermine the reputation of an EMB. When voter verification equipment, such as electronic poll books, are connected to the internet, compromise could lead to voter suppression or a voting disruption.[180] Because voter registration systems have public-facing components, such as information published online for public viewing, there is a risk that denial of services attacks can undermine voters and political party trust in the voter register, or in the election authority's credibility as a professional custodian of democratic elections.

Mitigation strategies:

- To mitigate these risks, **EMBs should disable remote access to these systems where possible.** (Note: this step may not be possible or necessary, if the voting public is able to proactively exercise functions online that must be authenticated and validated by the voter register database. For example, in the U.S. it is becoming increasingly common for voters to be able to request absentee ballots register to vote online.[181])
- **EMBs should employ designs that protect networks by using segmented protections.** This is akin to using multiple locked doorways in a long hallway, wherein each door provides an additional layer of security.
- **EMBs should use a third-party risk management process.** This means that as EMBs procure hardware, software, and services, they should formalize strategies to understand and address risk introduced by those third-party items and services. This includes the creation of policies and procedures governing vendor relationships, performing due diligence ahead of utilizing third-party services, and incorporating holistic strategies to limit identified risks.

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

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

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

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

- **EMBs should employ a patch management strategy that ensures timely closure of known vulnerabilities via updates issued by hardware and software providers.** Making sure hardware and software have the latest updates can quickly become a complex task across larger IT infrastructures. EMBs should ensure the task is approached strategically using industry good practice to identify assets most at risk to prioritize updates while keeping track of important metrics to track and improve performance in applying patches.[182]
- As specified in earlier sections, **EMBs should implement technical controls such as encryption for data in transit and at rest**; this is particularly important for biometric data that require more storage capabilities than demographic data.
- **EMB IT departments should work with the legal department to tailor managerial and operational controls that derive from local legal frameworks and requirements**, including ensure practices align with national and local laws around privacy protection and transparency obligations.
- **EMBs should also establish – through managerial and operational controls – business continuity and recovery plans** to ensure a quick, post-incident return to normal operations and clear contingency actions during cybersecurity events. When conducting field registration with standalone voter lists, the use of paper forms, in addition to direct field data entry, can serve as a hardcopy database backup in the event of data loss.

E. CANDIDATE REGISTRATION PROCESS

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

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

Risk discussion: Risk arises if adequate security, such as end-to-end encryption, is not utilized. A threat actor might compromise and change data to either disqualify contestants that have a legitimate ground to stand, or artificially allow contestants that do not. This can lead to election postponement, annulment or rerun, and, in some cases, electoral violence. There is also a risk that this personal information may become a target for various malign actors seeking to steal information for political purposes or financial gain. Where electronic registration mechanisms are used, the information that is printed on election ballots is often derived from the registration system. Ballot errors (or manipulations) can lend prima facie grounds for election annulment, hence making for an attractive cyber target.

Mitigation strategies:

- To mitigate these threats, **EMBs should implement the same sorts of controls discussed above that ensure network protection and encryption**.

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

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

F. EMB COMMUNICATIONS PLATFORMS

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

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

Mitigation strategies:

- The protection of privileged accounts is paramount to securing the online communication tools of EMBs; they must **use strong passwords and multi-factor authentication**.
- **Users should be trained to identify phishing and other social engineering techniques**, and they **should have different devices for different accounts when possible,** to prevent compromise of multiple communication channels.
- **Alternative communication plans should be prepared and tested well in advance**, and should include media, civil society organizations and political parties as partners in such planning and preparation. These considerations should be folded into the defined control set used within any implemented cybersecurity risk management program, likely falling within more traditional business continuity planning activities.

G. VOTER INFORMATION AND EDUCATION

Overview and main uses of technology: The provision of voter information and education is often a continuous process. Voter awareness of election-related issues ensures voters know when, where, why and how to vote. This bolsters voter confidence in the electoral process and helps voters make an informed choice. Tools and technologies vary by country context; while low tech solutions such as SMS campaigns, voice bots, or radio/podcasts are still used in rural areas, most countries are now using internet content, such as websites and YouTube channels. It is worth noting the exponential increase of the use of social media across the world, as a tool that has been adopted by most election administrations.

Risk discussion: Cybersecurity threats that may impact voter information and education efforts include denial of service attacks, which temporarily cut off public access to official sources of information about

the election. Additional threats are posed by disinformation campaigns, which can target audiences by compromising or taking over official electoral social media and email accounts, and websites.[183] Disinformation campaigns can also reach the public through creation of social media and email accounts and websites that are intended to mimic official sources of information on elections.[184]

Mitigation strategies:

- Legal frameworks can help mitigate some technological risks if local laws take into account such disinformation and enable enforcement activities. **Strong strategic and crisis communication plans and cyber hygiene awareness are effective and necessary**.
- **EMBs should establish contingencies, redundancies, and mitigation mechanisms** to ensure the continuous availability of services amid a breach by establishing pertinent controls within the larger risk management plan. For instance, EMBs should plan for public-facing resources to be mirrored on a separate provider's system so that those resources can be quickly re-deployed in the case of compromise or availability issues.
- **EMBs should also maintain relationships with social media platforms at the management level**, to more effectively detect and counter disinformation operations.

H. VOTING PROCESS

Overview and main uses of technology: On Election Day, a variety of technologies may be used in polling stations for the process of voting, including electronic or biometric voter authentication to confirm registration and/or identify voters, direct recording electronic (DRE) voting machines, optical scanners, or ballot marking devices (BMD).[185] Internet and absentee voting options are also part of this category

[183] In Cambodia in 2017 for example, the Facebook account for the Spokesman of the National Election Commission (NEC) was hacked and controlled by outside actors "for weeks," preventing accurate flow of information between the NEC, media and public. See Phnom Penh Post. (2017, October 9). *NEC Facebook Hack Investigated*. https://www.phnompenhpost.com/national/nec-facebook-hack-investigated

[184] In Georgia, for instance, a malicious actor set up a mock Facebook account named 'We are the Real CEC,' which mimicked the EMB's own Facebook page. This mock account was used to release false information (including a decree purportedly issued by the commissioner regarding election observers) and the content was reposted several times by other political actors. See International Society for Fair Elections and Democracy. (2021, September 28). *Manipulative Campaign on Facebook Regarding Election Processes*. https://isfed.ge/eng/sotsialuri-mediis-monitoringi/manipulatsiuri-kampania-Facebook-ze-saarchevno-protsesebtan-dakavshirebit; and FactCheck. (2021, September 28). *Fabricated Image of the CEC Chairperson's Decree Is Disseminated Through Social Networks.* https://factcheck.ge/en/story/39991-fabricated-image-of-the-cec-chairperson-s-decree-is-disseminated-through-social-networks

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

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

Risk discussion: Cybersecurity risks include physical hardware and software manipulation. DRE have been shown to be vulnerable to various types of potential attacks, including man-in-the-middle attacks,[187] which seek to change information or votes.[188] These have been proven successful in controlled attempts both within the United States and the Netherlands, and to some extent, their success has also led to a significant adjustment or roll-back of this technology in these and other countries. The danger for electronic voting machine (EVM) manipulations does not only stem from the machine's software, but also the hardware. Supply-chain risk management has become a major concern following a recent increase in globally-reaching attacks.[189] If a threat actor can gain access to an EVM while it is being transported or assembled, for instance, there are several ways the machine may be altered to facilitate vote manipulation.[190] A device could be inserted to take control of the unit, a chip that records the votes could be replaced with a fraudulent or malicious chip, or the software could be compromised before it is installed in the EVM to alter votes after they are entered but before they are recorded.

Remote access to internet-based voter verification systems, sometimes using biometric functionalities, is used to prevent multiple voting and facilitate absentee voting, presenting a risk of voter suppression if penetrated. There have been few reported cases where these systems cause polling delays and queues due to denial of services attacks, but there is growing concern about the potential impact of such attacks.[191]

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

---

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

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

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

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

[190] Hodgson et al. (2020).

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

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

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

Mitigation strategies:

- To effectively combat threats to electronic voting, **EMBs should implement controls that specify hardware- or firmware- level security settings that will help prevent manipulation.**
- **To mitigate third-party risk, EMBs should establish chains of custody, hardware inspections and efficient control of software and firmware hashes**.[194] External interfaces such as USB ports should be disabled if not in use; full disk encryption hardware such as laptops and voting machines should be mandated and utilized; and physical security measures such as locks should be employed to prevent possible manipulation or theft of equipment.
- **EMBs should consider security testing by independent parties**, either through code and hardware inspections, penetration testing or other evaluations.
- **The use of voter-verifiable paper audit trails (VVPAT)**, along with transparent and inclusive audit procedures, is considered an established good practice, and **is increasingly recommended** by election observers and technical assistance providers.
- **EMBs should also advocate for developing contingency plans within legal frameworks that address the possibility of compromised electronic voting technology**. The operationalization of paper ballot-based contingency plans can be extremely time-consuming and costly. Therefore, postponement and rerun may offer more affordable options in case of localized cyber attacks on limited numbers of EVMs
- **Holding extra voting machines in** reserve in case there is need for a replacement might also salvage an election in which a limited number of EVMs are compromised by cyber attack. Where VVPAT are available, legal frameworks must elaborate parallel procedures for counting and aggregated paper ballot receipts. This is discussed further in the counting section below.

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

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

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

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

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

I. COUNTING AT THE POLLING-STATION LEVEL

Overview and main uses of technology: Depending on a country's legal framework, the counting process may either take place directly after voting in individual polling stations, or at counting centers. However, currently a vast majority of countries count the votes at the polling-station level. A variety of technologies may be employed at this stage, including: scanners to process and tally voter choices on paper ballots; electronic machines that print ballot receipts that voters can check before they cast their ballot; and DRE machines that count votes without a paper record, or sometimes with a QR code that voters can check. If any vulnerabilities are exploited at this stage of the process, it can lead to questions about the integrity of electoral results and fundamentally undermine public confidence.

Risk discussion: The cybersecurity risks associated with the counting process include manipulation of hardware or software (by trusted or untrusted actors) to modify results. In several proof of concept demonstrations, ballot scanners have been exploited to modify the results of an election while leaving virtually no detectable trace of fraud.[198] The recent compromise of the software provider SolarWinds displayed how mundane software tools and the application of updates can be a vector for sophisticated attack.[199] Hardware and software utilized at polling stations, even if relying on bespoke solutions, may still be exposed to threats emanating from determined adversaries that have infiltrated the supply chain of supporting or secondary infrastructure.

Mitigation strategies:

- **All ICT devices present or used in the counting process should be *hardened*** – the process of securing a server or computer system by minimizing the attack surface. Hardening includes both physical and software measures to prevent unauthorized access and manipulation. **When EMBs purchase equipment, appropriate security tests should be utilized to define what hardening procedures should be applied** to systems beyond the manufacturer's configuration. **These procedures should be maintained and updated** as appropriate as part of the holistic risk management program.[200]

---

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

- As covered earlier, **EMBs should obtain software and firmware hashes from manufacturers** to ensure that devices and software have not been altered and that they are verifiably genuine.
- **All devices should be certified before use**.
- **ICT devices should all use universal BIOS/UEFI security settings** to prevent manipulation and tampering.[201] When not in use, all USB ports, WIFI and Bluetooth should be disabled.
- Ideally, the ICT systems used for the counting process should be **housed in an enclosed case and have full disk encryption enabled**.[202]
- **EMBs should establish and maintain the proper chain of custody for transporting and storing the equipment**.
- **Tabulation audits are also integral to the mitigation strategy for lapses introduced during the counting process**, as discussed in greater depth in the literature review, legal framework and results transmission sections of this report.

J. RESULTS TRANSMISSION, TABULATION AND REPORTING

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

Risk discussion: Attacks on results transmission and tabulation systems are a common tactic for actors seeking to undermine trust in elections. Such attacks may seek to alter vote counts or create public confusion and doubt about the integrity of an election's outcome. DDoS (distributed denial of service) attacks may also be staged at this phase of an election - preventing public access to results sites by overloading it with requests originating from a botnet.[203] Along with attacks on elections systems and websites, disinformation campaigns pose a major threat in the post-election period. Release of false

---

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

[202] "Full disk encryption is a cryptographic method that applies encryption to the entire hard drive including data, files, the operating system and software programs." See Ford, A. And L. Huthinson. (2016, January 16). *Full Disk Encryption: Do We Need It?* CSO. https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html

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

information about preliminary and final vote counts may seek to create doubt about the validity of election results, or to elevate social tension and strife.

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

In 2018, Iraq began using ballot scanners that were expected to transmit results through the mobile phone network. The results of those ballot scanners that were used outside mobile phone coverage areas were loaded on USB memory sticks that were physically transported to regional results centers. Several such USB devices were reportedly intercepted and manipulated. The results data was changed, so that it no longer aligned with the scanned ballots in the ballot box.[204]

Mitigation strategies:

- As discussed earlier in this paper, **tabulation audits** – including both fixed percentage and risk-limiting audits – are an important mechanism for ensuring the credibility and trustworthiness of technology-driven count and results processes.[205]

A Caveat On Tabulation Audits

As IFES has noted previously, tabulation audits fundamentally require verifiable paper records of the intent of voters – to ensure an independent record of the votes cast to assess the accuracy of a tabulation system's results. Some DREs produce a paper receipt that can be used as part of the audit trail. In India, for example, the Supreme Court ruled that all voting machines must be equipped with printers to provide voter- verifiable paper audit trails (VVPAT) to allow each voter to verify that his or her intended selections are correctly printed on a paper record, which is collected in a separate container called the VVPAT box."[206]

Such audits are also inherently limited in their ability to detect errors or incursions occurring in the voting system prior to the initial count. As Verified Voting has noted about risk-limiting audits in particular, "[they] are one piece of the larger ecosystem of evidence-based elections that depend upon a trustworthy record to give confidence to election outcomes. ... They do not tell us whether the voting system has been hacked. They do not and cannot determine whether voters actually verified their ballots. But they can detect and correct tabulation errors that could alter election outcomes..."[207]

- **Complementary procedures and compliance checks are needed that ensure that the paper and electronic records used in a tabulation audit are fully secured**, including poll

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

book accounting to compare the number of voters with ballots cast; ballot accounting to reconcile the number of ballots distributed with the number of ballots cast and the number of blank or spoiled ballots returned; reconciliation of votes to check mathematical accuracy of tabulation forms; chain of custody checks to review signature logs and ensure custody of all secure election materials; and security checks to ensure that ballots and boxes have been protected with tamper-evident seals and other security features.[208] Proper chain of custody in particular "is a crucial component of investigation and dispute resolution, more generally, as adjudication decisions may be affected by the quality of the physical evidence supporting a complaint."[209] Compliance checks are also valuable in the event of a court challenge against the results.

- It is similarly important that the EMB makes every effort to **centrally retain a full set of the official paper-based results forms** for verification of results, or recounts, should a court of law order one or if the legal framework contains triggers for one**.** In 2017, the Kenyan EMB relied so heavily on its electronic results transmission system, KIEMS, that it neglected to centrally collect and verify the original signed paper results sheets before releasing results. In absence of a full record of all polling station results forms justifying the EMB's national results announcement, the Supreme Court (constrained by a 2-week deliberation period) saw no other option than to annul the election nationwide.
- **Wi-Fi functionality and Bluetooth should be disabled when not in use** and controlled through use of standardized and managed hardware and software configuration policies.
- **Hardware should be procured with requirements to limit functionality to only the necessary components.**[210]
- As with the IT infrastructure discussed in earlier sections, **end-to-end encryption**[211] must be used to ensure integrity of the data in transit and at rest. **Proper cryptographic methods** must be used to authenticate clients (for the data entry of results) and servers (to the centralization). Further, **EMBs should use dedicated, offline, and/or encrypted infrastructure**.

K. ELECTORAL DISPUTE RESOLUTION PROCESS

Overview and main uses of technology: Effective resolution of electoral complaints is essential to the integrity and legitimacy of an election. Increasingly, election dispute resolution (EDR) bodies use technology as part of the complaints adjudication processes. For example, many forums accept complaints through online channels, some online portals allow the uploading of electronic evidence, hearings are increasingly being held remotely, and EMBs and EDR tribunals are also increasingly relying on electronic case management systems.[212]

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

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

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

Mitigation strategies:

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

L. DETECTING, INVESTIGATING AND PROSECUTING CYBERCRIME IN ELECTIONS

Overview and main uses of technology: Malicious activity involving a computer, computer network or a networked device to conduct a criminal act is known as a *cybercrime*. A range of cyber attacks, including hacking voter databases, tampering with voting machines, denial of service attacks or theft of data for information operations in elections could represent a cybercrime under national legal frameworks and the 2001 Budapest Convention.[213] While a major focus of governments is necessarily protecting networks from attack, this may not be a sufficient deterrent against future attack, and the detection, investigation and prosecution of cybercrime in elections remains important. When it comes to cyber attacks against elections, the Venice Commission concludes that, "greater efforts need to be undertaken to prosecute such interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections."[214]

Risk discussion: Cyber attacks against elections have so far yielded few arrests. In 2020, a man was arrested for perpetrating distributed denial of service attacks against the website of a congressional

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

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

candidate in California.[215] There are many challenges to detecting, investigating, and prosecuting cybercrime in elections. This includes challenges around jurisdiction, and the need for international legal cooperation where such crimes are cross-border. For example, the Russian Federation refuses to extradite its citizens to foreign states on cyber crime charges and is not a signatory to the 2001 Budapest Convention. As a response, the European Union has placed targeted sanctions on the suspects.[216] The United States government made its first indictment against foreign election cyber attackers in 2018 but was not able to take custody of the 12 suspects.[217] A second challenge is anonymity, and the tension between detecting perpetrators of cyber-crime while protecting privacy rights. Finally, evidence in cybercrime cases can be a challenge, as it is often fragile and easily destroyed. It can also be difficult to maintain a chain of custody. All these challenges put the investigation and prosecution of cybercrime at risk.

Mitigation strategies:

In 2020, IFES issued the Election Investigations Guidebook—Standards, Techniques and Resources for Investigating Disputes in Elections (STRIDE), which advises EMBs and investigators on principles for detecting and combating electoral offenses, in line with international standards.[218]

- **It is imperative that EMBs and investigators be able to secure electronic evidence**, and where necessary cooperate with a range of domestic agencies and international law enforcement personnel under the Budapest Convention **to identify and prosecute offenders** (and to secure evidence that may be in other jurisdictions).
- **There may also be a need to cooperate with service providers on both protecting and accessing evidence**. In 2019, the United Nations Office on Drugs and Crime (UNODC) department on cyber-crime published its Training Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns & Warfare in Cyberspace, Information Warfare, Disinformation & Electoral Fraud. [219]
- In the spirit of the Budapest Convention, **EMBs may also consider initiating peer platforms for information and good practice sharing, and international emergency hotlines in the realm of detecting and investigating cyber-attacks on elections**.
- Similar to the civil society context, high profile political targets will not be protected by basic cyber-hygiene practices. As demonstrated by the Pegasus leak,[220] some countries will use surveillance tools to monitor activities of political opposition. **High profile political targets could call upon specialized agencies to secure their devices, otherwise they should consider them compromised**. The objectives of the national or foreign state targeting high profile targets will usually be discrediting or acquiring information that can be used for blackmail.

---

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

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

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

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

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

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