USAID
FROM THE AMERICAN PEOPLE

Briefing Paper: Cybersecurity and Voter Registration

BIOMETRIC VOTER REGISTRATION IN KENYA, PHOTO PROVIDED BY IFES.

JULY 2022

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

Acknowledgements

This paper was prepared by the International Foundation for Electoral Systems (IFES) Center for Applied Research & Learning in consultation with DAI and USAID's Center for Democracy, Human Rights and Governance (DRG Center). Thomas Chanussot and Dr. Tarun Chaudhary were the lead authors. The paper benefited tremendously from contributions by Matt Bailey, Dr. Staffan Darnolf, Erica Shein, Dr. Fernanda Buril, Veronika Prochko, and Annie Styles. The team is grateful to those individuals who reviewed various drafts and provided valuable insights.

DISCLAIMER This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of DAI and do not necessarily reflect the views of USAID or the United States Government. This publication was produced under DAI's Digital Frontiers Project (Cooperative Agreement AID-OAA-A-17-00033) at the request of USAID.

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

CONTENTS

Section I: Introduction

This briefing paper was developed for the United States Agency for International Development's Democracy, Human Rights, and Governance Center (USAID DRG) to inform a broad audience, including USAID DRG personnel, implementing partners, and local electoral stakeholders on voter registration and cybersecurity issues.

Citizens' right to participate in public affairs is a cornerstone of democracy, and voter registration (VR) is a crucial to achieving that participation.[1] A quality registration process helps to enfranchise eligible voters. Similarly, a flawed registration process can have the opposite effect, causing the legitimacy of an entire election to be undermined.

Balancing Rigor and Flexibility in Voter Registration

"Electoral rolls are a fundamental component of any voting system. Rolls constitute the official list of electors and are prima facie evidence of electors' right to vote. Enrolment procedures therefore need to strike the right balance between the need to be rigorous to ensure integrity of the rolls, and the need for flexibility to ensure that peoples' rights to enroll and vote are protected."[2]

- The Electoral and Administrative Review Commission of Queensland

A credible voter list has four key characteristics. It must be **transparent**, making it easy for a person to register to vote; **comprehensive**, to guarantee that all groups of eligible citizens are registered; **accurate**, to ensure that the information allows officials to find voters on the list and eliminate any duplicate registrations; and **current,** to reflect changes in the population. The latter requires the list to be rigorously maintained by the relevant authorities.

Voter registration is often the most resource-consuming activity in the electoral process, sometimes accounting for more than fifty percent of the overall cost of administering elections.[3] The high costs are largely due to the technologies used by the administrative body (or bodies) responsible for voter registration, but personnel costs, logistics, training, and voter education efforts are also significant expenses.[4] Throughout the last two decades, EMBs have increasingly complemented paper-based registration methodologies with digital ones, creating national voter registration databases. Voter

[1] See Article 25 of the International Covenant on Civil and Political Rights, December 16, 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights?ftag=MSF0951a18

[2] Electoral and Administrative Review Commission of Queensland, Australia. (1992). *Report on the Review of the Elections Act 1983-1991and Related Matters, vol.1.* (p. 46). https://documents.parliament.qld.gov.au/tableoffice/tabledpapers/1992/4692T1506.pdf

[3] Neufeld, Harry. (1997). The Range of Advanced Technologies Available for Election Organizations. In Carl W. Dundas (Ed.), *Let's Talk About Elections* (p. 58). Commonwealth.

[4] For more detailed information regarding election costs, see UNDP & IFES. (2005). *Getting to the Core: A Global Survey on the Cost of Registration and Elections*. https://aceproject.org/ero-en/misc/undp-ifes-getting-to-the-core-a-global-survey-on/view; also useful, data available at: IFES. (n.d.). Pricing in Elections. https://www.pricinginelections.org/ExploreTheData/

PERSONALLY IDENTIFIABLE INFORMATION, OR PII

As defined by the National Institute for Standards and Technology's Computer Security Resource Center, Personally Identifiable Information, or PII, is:

"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[5]

PII may include names, addresses and contact details, dates of birth, and unique identification numbers.

registration databases allow an EMB to identify errors and fraud in voter lists and contribute to faster updating and printing of voter registers. However, they also generally include biometric data and other forms of personally identifiable information (PII) and can present unique cybersecurity, surveillance, and governance risks.

To ensure modern, high quality, and secure elections, EMBs must stay up to date on their understanding of voter registration technologies and the rapidly increasing and evolving use of tech in the sectors that affect electoral environments. They must also be aware of the public's growing expectations for online governmental services that match the quality and ease of commercial ones.

The COVID-19 pandemic only increased the urgency of this issue, as more government services were made available online. EMBs are under increasing pressure to deploy more technology faster, causing systems and data to be increasingly exposed in an ever more dangerous online environment. These trends make it critical for them to enhance their internal information and communication technology (ICT) capacities and cybersecurity expertise to protect against internal mistakes and maladministration, as well as external threats that impact voter registration processes, the personal data at play, and voter lists.

The good news is that while these challenges are new to the elections space, they have been studied within the larger government cybersecurity community for some time and there are frameworks that can be adapted to help secure voter registration as it is brought online and as new threats emerge.

Essentially, cybersecurity can be defined using the basic concepts of *confidentiality*, *integrity*, and *availability* of information.

- Confidentiality means ensuring the data is only accessed by authorized users for intended purposes.
- Integrity means ensuring data is not altered inappropriately.
- Availability means the data can be accessed whenever needed and is not subject to deletion, outages, or similar issues.

Ensuring the cybersecurity of a VR process involves assessing and limiting risks related to the confidentiality, integrity, and availability of its systems and data; it is as much a governance issue as a technical one. VR cybersecurity risks can be managed through a combination of policies, education of users and managers involved in voter registration activities, and the application of technology.[6]

[5] National Institute of Standards and Technology (NIST). (n.d.). Glossary: PII. https://csrc.nist.gov/glossary/term/PII

[6] For further information about cybersecurity and the electoral process see: Primer: Cybersecurity and Elections available from USAID.

Voter registration stands out from other processes where interaction between the government and citizens is required because citizens' identities must be validated at some points in the voting process but kept anonymous during others. This is in addition to preventing against manipulation or mismanagement of PII. For instance, while a census affects all residents of a country as the authorities collect data about them, personal information such as name and biometric data are excluded. Tax collection, however, generally includes significant amounts of PII but does not require records to be anonymized as they are processed or audited.

On election days, officials are increasingly cross-checking voters' identities against existing databases using a voter's cards or other forms of official identification, but they rarely collect biometric information at the polls. During voter registration, on the other hand, it is increasingly common for officials to collect and link individuals' personal information, biometric data, home addresses, and family ties into one database, often rendering it a nation's most sensitive database of PII. To instill confidence in the voter lists and to identify errors in them, the election authority must make provisional voter lists easily accessible to the electorate and political parties. By enabling online searches, mobile applications, and SMS-solutions to access voter registration information, EMBs have greatly enhanced voter lists' transparency. But in doing so they have also increased potential exposure to bad actors looking to breach or misuse such databases for nefarious purposes.

A range of bad actors around the world are taking advantage of underinvestment in cybersecurity to attack democratic systems. Voter registration and other electoral management systems are no exception. The motivation behind these attacks varies, from simple mischief to undermining or manipulating the voter registration process for political aims, to personal data theft for financial gain. Numerous incidents have been reported worldwide, with different degrees of impact. There have been a number of breaches and exploitation of poorly protected voter databases or vendors to date.[7] Attacks on physical devices used to capture voter information, such as USB keys, have also been reported.[8]

To date, attacks on voter registration systems do not appear to have fundamentally undermined election results, but the increasing sophistication of attackers and the increased deployment of voter registration technology means that future attacks could have greater impacts. For example, documented failures of biometric voter registration systems to prevent duplicate registration, and systems that have failed to consistently identify voters correctly at the polls show that intentionally creating such errors on a large enough scale could undermine electoral outcomes.[9] Such instances have damaged the credibility of EMBs, sometimes triggering a legal response from watchdog organizations, and even reducing public confidence

[7] For an example, see the following: Degler, Andrii. (2016, April 25). *Millions of Mexican voter records leaked to Amazon's cloud, says infosec expert.* Ars Technica. https://arstechnica.com/information-technology/2016/04/millions-of-mexican-voter-records-leaked-amazon-cloud/; and Temperton, James (2016, April 22). *Massive Philippines Data breach now searchable online.* Wired. https://www.wired.co.uk/article/philippines-data-breach-comelec-searchable-website

[8] Kang-chung, Ng. (2017, June 12). *Hong Kong privacy watchdog blasts electoral office for massive data breach.* South China Morning Post. https://www.scmp.com/news/hong-kong/politics/article/2098002/hong-kong-privacy-watchdog-blasts-electoral-office-massive

[9] See, for example, the case of Uganda, Ghana, and Kenya detailed in: Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. *Democratization*, *25*(8), 1397-1418.

in the electoral process in some cases.[10] A 2021 survey on democracy in the EU reported that 57 percent of respondents were *"concerned about the elections being manipulated through cyberattacks."*[11]

Apart from this potential abuse of data within voter registration databases to disenfranchise targeted groups, the information can also be used in influence operations[12] or even to generate lists of opposition affiliated voters to target with some form of violence. What's more, even the public *perception* of possible abuses of voter lists by malicious actors can undermine trust in elections and influence voter participation, including in countries where such abuses have not been documented.

This briefing paper includes the following sections:

- Section II of this paper provides an overview of key technologies and data that are at risk throughout different phases of the voter registration process;
- Section III introduces the different types of threat actors that may target election processes and their potential motives for attacking voter registration;
- Section IV analyzes the risks and impacts of cyberattacks on the voter registration process;
- Section V describes the techniques, tactics, and procedures used by threat actors; and
- Section VI outlines possible mitigation measures to reduce cybersecurity risks.

Section II: Overview of VR Technologies and Processes

Voter registration is a complex process. Domestic politics, culture, geopolitical context, and the legal mandate, budget, and technical maturity of the EMB all have an impact on the tools and technologies adopted for elections. When considering voter registration technology and cybersecurity, EMBs need to address a number of questions that shape how the process unfolds in their jurisdictions:

- *Should voter registration be mandatory or voluntary?*
- *Should registration be proactively pursued by sending registration officers house-to-house or should registrants be required to show up in person at registration centers?*
- *What types of identification documents are necessary for registration and what form of proof will be issued upon registration (e.g., voting card, electronic record linked to biometric info, etc.)?*
- *Should the voter list be continuous (updated on a rolling basis) or periodic (created anew at some interval)?*
- *Can the voter list be extracted from the civil registry?*
- *Would biometric voter registration help ensure the list is trusted by stakeholders?*
- *Should the list be under centralized or decentralized management?*
- *How will the provisional voter list be displayed, and how can voters make corrections and update registration information?*

[10] The chairman of the COMELEC was prosecuted over the database leak: ABS-CBN News. (2017, Jan 5). *Comelec's Bautista faces criminal raps over massive data leak.* https://news.abs-cbn.com/news/01/05/17/comelecs-bautista-faces-criminal-raps-over-massive-data-leak

[11] European Union. (2020): *Democracy in the EU.* (Special Eurobarometer 507) [Data Set]. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=74250

[12] Influence operations "…are organized attempts to achieve a specific effect among a target audience." See, Elise et al. (2020, June 10). *The Challenges of Countering Influence Operations.* https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031

The local legal framework, and the electoral law in particular, will impact the technology used and how the integrity of the list is protected.

A. CAPTURING VOTER INFORMATION

There are three common voter registration models:

- *Periodic voter lists* are created anew by EMBs for each election. Lists are not maintained or updated for subsequent election cycles.
- *Continuous registries* are used across election cycles, and are updated by EMBs as new voters are registered, registered voters move, and voters who are no longer eligible to vote or have died are removed. These registries are then used to produce voter lists.
- *Civil registries* are automatically pulled from existing databases – such as national ID card systems and passport databases – maintained by state institutions, such as tax authorities, municipal authorities, or interior ministries. With this process, EMBs have less responsibility and control over the quality of the voter lists they create that leverage the state civil registry.[13]

Depending on which model a country uses, voter registration processes will look very different. However, a common list of tools used across these models can be found below.

COMMON TOOLS FOR VOTER REGISTRATION DATA COLLECTION	
DIGITAL DATA CAPTURE	NON-DIGITAL DATA CAPTURE
○ Digital cameras ○ Fingerprint scanners ○ Iris scanners ○ Computers & tablets (with digital forms) ○ Document scanners	○ Polaroid cameras ○ Paper forms such as ledgers, registration forms, affidavits, witness statements and other required information (these can potentially be fed into scanners to digitize) ○ Fingerprint ink and pads

Periodic and continuous voter lists might use biometric devices to capture fingerprints, iris scans,[14] and digital photos. These three forms of biometrics are unique to every individual, and, along with other personal details, they are stored in the computer used to produce the voter register. The main benefit of biometric voter registration (BVR) is its ability to detect and flag, as well as deter, multiple registrations. Biometric data is also used to identify voters at polling stations,[15] and network-connected biometric

[13] A more detailed review of the pros and cons of the types of voter registration processes can be found on the ACE Project website -ACE Project: The Electoral Knowledge Network. (n.d.). *Voter Registration*. https://aceproject.org/ace-en/topics/vr/default

[14] Though less common than fingerprints and digital photos, Somaliland and Puntland have both used iris scans successfully in recent elections. For information about their use in Somaliland, see: Schueller, M. L., & Walls, M. (2017). Reports by international observers on the 2016 voter registration process in Somaliland. *Progressio*; IFES assisted the Transitional Puntland Electoral Commission (TPEC) in evaluating voter registration options and designing its voter registration solutions for the 2021 local council elections. In the end, TPEC used a combination of biometric data, including iris scans. For further details, see the Transitional Puntland Electoral Commission website at https://tpec.pl.so

[15] International Institute for Democracy and Electoral Assistance (International IDEA). (n.d.). *Is The Biometric Data in Voter Identification at Polling Stations?* https://www.idea.int/data-tools/question-view/739

verification devices can be used to prevent an individual from casting a ballot at multiple locations on election day.

Today, many countries collect non-biometric voter information (such as name, address, sex/gender, date of birth) directly via laptops and tablets at registration centers. Alternately, data clerks may collect voter data via paper forms, which are then scanned and digitized, or manually entered into databases. Finally, a very small number of countries still use handwritten voter list ledgers to create the voter list, such as Ethiopia during its most recent 2021 general elections. In this process, voter data may never be digitized.

Personal Data in Elections: Balancing Transparency and Privacy of Voter Information

A necessary balance between voter registration process transparency and the protection of citizens' privacy must be struck.

The voter list should be public. Elections stakeholders should be able to consult the data to ensure it is accurate and aligns with international election standards. Most election laws require EMBs to publish the voter list in a way that is accessible to public scrutiny.[16] On the other hand, voters are entitled to privacy, with some exceptions; there is a global trend toward a data privacy protection legal framework. The European General Data Protection Regulation (GDPR), for example, strictly frames the use of data, including lists of citizens that are used to compile voter lists.[17] If the list is used for any other purpose, administrations must notify and collect consent from the voters.

EMBs and other election stakeholders must make tradeoffs in service of either transparency or voter privacy. Countries have approached these tradeoffs in a variety of ways. Some countries like North Macedonia have begun aligning their data privacy legal framework to incorporate GDPR requirements to facilitate commerce with the EU.[18] However, the State Election Commission (SEC) is exempt and is not required to apply data protection measures that would otherwise be required for personal data such as the voter list. Since the application of privacy protections falls within the purview of cybersecurity management, EMBs are likely to incorporate new parameters to their cybersecurity program requirements that comply with both electoral and data protection law.[19]

[16] United Nations Committee on Human Rights. (1996). General Comment 25, "The Right to Participate in Public Affairs, Voting Rights and the Right to Equal Access to Public Service." https://www.osce.org/odihr/elections/19154

[17] European Commission. *Data Protection: Rules for the protection of personal data inside and outside the EU.* https://ec.europa.eu/info/law/law-topic/data-protection_en

[18] Office for Democratic Institutions and Human Rights (OSCE). (2021). Republic of North Macedonia Local Elections 17 and 31 October 2021 ODIHR Election Observation Mission Final Report. (pp. 12-13).

[19] Privacy International. (2019, June). *Technology, data and elections: A 'checklist' on the election cycle*. (pp. 5-8). https://privacyinternational.org/sites/default/files/2019-07/Technology%2C%20data%2C%20and%20elections_0.pdf

B. STORING, TRANSFERRING, AND PROCESSING VOTER INFORMATION

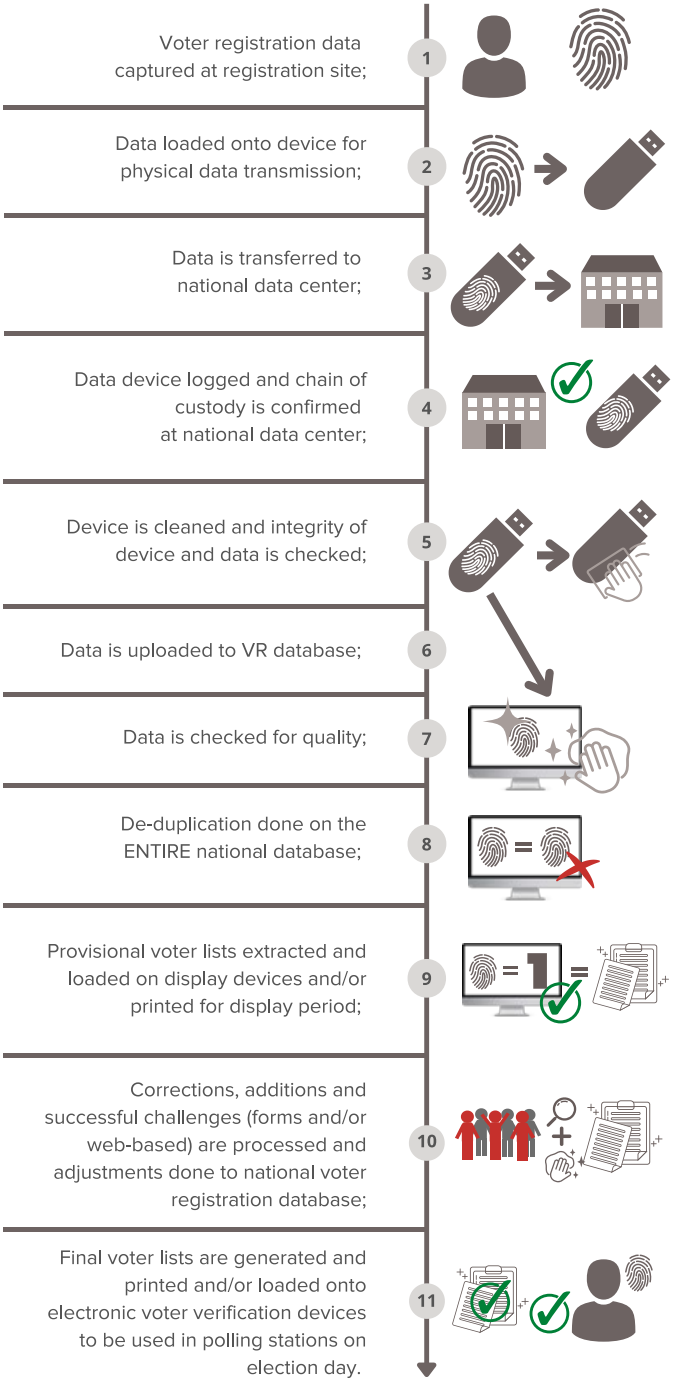
Common Tools for Physical Data Transmission

- USB flash drives
- Portable hard drives
- Mobile cellular devices

EMBs generally seek to consolidate VR and other data in a central system or storage service, rather than leaving it distributed across devices, services, or offices. The benefit of data consolidation is that it helps to ensure that each eligible voter is only registered once. It also helps detect and deter fraud, as well as make corrections and ensure accuracy. Most countries centralize voter registration data after the initial data capture, though some have struggled to complete this labor-intensive process.

The transfer of voter information to a central database, whether directly or through a series of processes and systems, can be done electronically or via a physical device, such as a flash disk, a portable hard drive, or the laptop computer used to collect the data. Like other online communications, electronic transfer can occur over a network connection, and may require a mobile cellular device to connect to the Internet such as mobile phone, mobile Internet "hot spot" or wireless USB device that is plugged into a laptop using a local Internet connection. This approach can be appropriate but, as with any process that involves an Internet connection, it raises numerous security concerns related to confidentiality, integrity, and the availability of the data being transmitted. Transfer done via network connections must be secured via encryption, among other measures. When registration data is transferred via physical devices, such as USB drives, they must be properly screened for malware prior to being connected to the central voter registration system. This can be a significant logistical consideration, as sometimes there are thousands of them. In some instances, screening for malware is achieved by using an "air

FIGURE 1: STEPS TO UTILIZE VOTER DATA



gapped" computer (i.e., one that is not connected to a network) for initial checks of portable devices and their content. Whether data is transferred electronically or physically, it should always be checked for integrity to ensure the data received is the same as the data initially captured for transfer.

When voter lists are created from civil registries, several databases are usually combined to obtain the final list of eligible voters. The process can be semi-automated or fully automated, depending on the number of databases and the maturity of the information systems involved. Ultimately, the data extracted from civil registries is transferred electronically or physically to an EMB data center or other centrally controlled location. Some countries also interconnect datasets, allowing the EMB to verify voter information collected by their agents against the national ID database.

Detecting duplicate voters (using biometric and/or demographic data) is the main advantage of centralizing data. Duplicate records are usually flagged for review by a human operator, a process called adjudication. Innovative solutions can also be integrated during this stage to reduce fraud.[20] In Guinea-Conakry, for example, algorithms have been put in place to detect and remove children from the roll based on their facial features.[21] Solutions using or touting technology such as artificial intelligence, machine learning, "algorithms," and predictive analytics should, however, be used with caution as they can be difficult to design free of bias and with appropriate levels of rigor and accountability.

A number of processes must be executed across the collection of data represented by the voter registration database records. This requires a large amount of computer processing power and data storage. These include, for example, deduplicating/matching biometric records, and writing and executing large queries that result in unique lists of voters sent to polling stations that are often also printed and distributed according to legal deadlines, along with other computing intensive tasks. EMBs have to invest in powerful and expensive servers and equipment to ensure all activities can be conducted on time. Some may outsource the process to cloud-based infrastructure, sometimes in other countries. Due to the highly technical skillset required during this process, EMBs may rely on external service providers or consultants, providing them with privileged[22] access to highly sensitive data. Such external services may need additional configuration to adequately protect data. Integrating third-party services into one's own cybersecurity program may require sophisticated skillsets and should not be done without due consideration.[23]

Where EMBs decide to build their own data centers to house voter registration information, a number of concerns must be addressed and good practices applied. Such "on-premise" solutions require, for example, adequate power with back-ups, physical security, and redundant infrastructure at a secondary location, along with technical staffing proficient at troubleshooting and fixing issues as they occur. Beyond standard information technology concerns, further cybersecurity-based protections should include both

[20] Wolf, P., Alim, A., Kasaro, B., Namugera, P., Saneem, M., & Zorigt, T. (2017). *Introducing biometric technology in elections*. International Institute for Democracy and Electoral Assistance (International IDEA). https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf

[21] Kapusta, Matus. (2020 September 21). ID4Africa LiveCast: Innovatrics Face Recognition Cleans Guinea's Voter List from Duplicates and Minors. https://www.innovatrics.com/news/id4africa-livecast-innovatrics-face-recognition-cleans-guineas-voter-list-from-duplicates-minors/

[22] Privileged access is an information technology term that denotes elevated rights to access sensitive data and systems. Often access is controlled by designating certain categories of users as having elevated privileges (user rights) on specific systems or to specific data.

[23] In 2016, the personal information of 93.4 million Mexican citizens was exposed after a misconfigured database was found on Amazon Web Service by security researchers. More information can be found at: Cameron, Dell. (2016, April 22). Private records of 93.4 million Mexican voters exposed in data breach. Daily Dot. https://www.dailydot.com/debug/amazon-mexican-voting-records/

physical and digital security measures, robust access control, and logging solutions[24] to enable forensic audits and investigation during cybersecurity incident response. These are a sampling of the many necessary components involved in data center operations.

C. USING VOTER INFORMATION DURING THE ELECTORAL PROCESS

Voter List Verification

Having collected and processed the voter registration data, EMBs compile preliminary voter lists, receive corrections and complaints, and reconcile these into a final voter list.

Preliminary voter lists serve multiple purposes. For instance, they allow voters to ensure that their personal information is correct and registered at the appropriate polling station; they may be shared with parties and candidates to inform campaigning; and parties and candidates may use these voter lists to audit for fraud and errors in voter registration. Traditionally, voter lists were physically posted in public venues. This practice is no longer commonplace because of privacy concerns and printing costs, and the necessary training and deployment of thousands of officers to manage voter lists display centers. In post-conflict societies, these factors are especially burdensome.[25] Alternatively, online lists and services to provide access to them have become more common. However, EMBs, like other ministries and governmental bodies, continue to struggle in this area; the deployment rates of digital voter lists have been slow and vary in quality.

Several countries have also used low-tech approaches to reach a large number of citizens with no or low Internet connectivity. Tunisia, for example, used SMS as a verification mechanism until 2019.[26] In 2014 and 2021, voters in Libya registered using a coded SMS, which included their private information and addresses. Their polling locations and verification codes were sent to them in response to the SMS.[27] A number of countries now rely on web technologies (websites, smartphone applications) to provide voter verification services. Voters can go online and enter private information, usually their name and their date of birth or their national identification number, to obtain their voter registration information or where they are registered to vote.

Other countries have deployed extensive self-service mechanisms, allowing users to authenticate and directly interact with the election administration to manage their voter record. This interactivity goes beyond simply looking up registration status and adds a layer of complexity to ensure infrastructure security. India, for example, has a voter registration portal[28] that allows individuals to register, declare any

---

[24] Logging is an information technology and cybersecurity term that refers to the act of capturing data related to activities performed on and with data during storage, processing, and transfer for the purpose of troubleshooting or investigation. Often this includes keeping track of who accessed what data when, assigning timestamps to various other actions and storing a record of when data was changed, added, or deleted along with other relevant "meta-data".

[25] ACE Project: The Electoral Knowledge Network. (n.d.). *Voter Registration*. https://aceproject.org/ace-en/topics/vr/vrb/vrb12

[26] The Carter Center. (2019). *2019 Presidential and Parliamentary Elections in Tunisia: Final Report.* (p. 33). https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/tunisia-2019-final-report.pdf

[27] More information about the SMS voter registration system deployed by the company CaktusGroup in 2014: CaktusGroup. (n.d.). *World's First SMS Voter Registration System*. https://www.caktusgroup.com/case-study/worlds-first-sms-voter-registration-system/

[28] Election Commission of India. *Voter Portal.* https://voterportal.eci.gov.in/

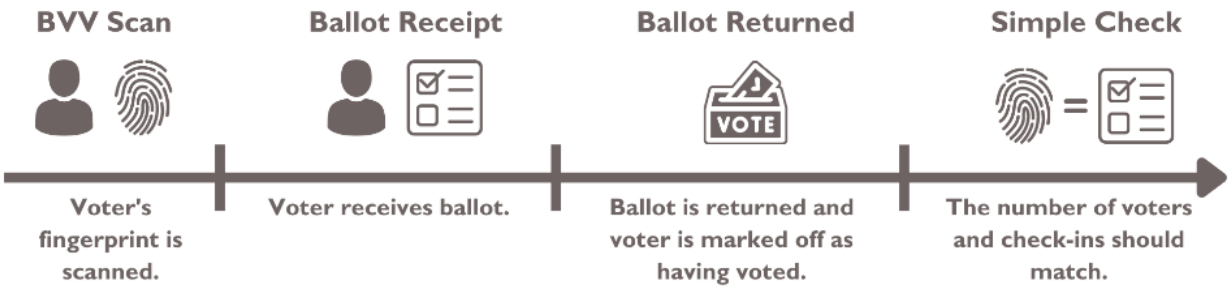
change of address, and share other relevant information with the Election Commission of India. A similar voter registration service is offered by the South African election commission.[29]

After addressing corrections to voter registration records that can sometimes number in the hundreds of thousands and any outstanding complaints about potential fraud, the EMB revises its preliminary voter list and creates a final one. As with other parts of the process, these steps must be performed under severe time constraints and can potentially involve judicial proceedings that can add further complexity. EMBs traditionally provide the finalized voter list to polling station officials in the form of a paper-based voter list for use on election day**.** Physical voter lists are still used in most countries. This is often acknowledged as a strength, as it limits cybersecurity risks, but it also makes errors harder to fix after printing.

Voter Verification and Voter List Technology on Election Day

On election-day, voter identity is verified against the final voter list. As with voter registration, countries use a variety of digital and non-digital processes to do so. Some may be as simple as verbal, a manual verification of the voter's voter card or national ID card, and others may involve cutting-edge technology.

FIGURE 2: BIOMETRIC VOTER VERIFICATION (BVV)



To reduce the risk of impersonation, multiple voting or blatant ballot-box stuffing by poll workers, an increasing number of countries are introducing various biometric solutions for identity verification – often called biometric voter verification (BVV) or biometric voter authentication (BVA). Polling stations are sometimes issued computers, tablets or other mobile biometric devices preloaded with the polling station's voter list, including their biometric data. For example, upon entry into a polling station, voters' fingerprints or faces are scanned by polling station officials to verify their identity against the voter list's biometric data record, preventing impersonation. As noted above and explored in more detail below, these approaches can offer benefits for voting security but can come with tradeoffs regarding cybersecurity and privacy.

[29] Election Commission of South Africa (IEC). *VoterPortal.* https://registertovote.elections.org.za/Welcome

Once the voter's identity is verified, the voter is issued a ballot paper for marking in secrecy and subsequently deposits it into a ballot box. Their name is then marked off the voter list as having voted. At the end of polling, presiding officers are usually required to compare the number of voters marked off with ballots found in the ballot box to minimize the risk for ballot-box stuffing.

An Example: Leveraging Biometric Data on Election Day

At the onset of Afghanistan's 2019 elections, the government had not yet established a baseline biometric database for registered voters – meaning they could not leverage biometric data to remove duplicate registrants from voter lists in advance of polling. Instead, digital photos and fingerprints were captured from voters on election-day itself before each individual received a ballot. These ballots were marked with unique QR codes. Biometric data, associated with unique QR codes, was then fed into a biometric matching system after the election and before the counting of the votes. Any evidence of multiple voting (i.e., identification of cases where identical biometric data was associated with more than one unique QR code) was referred to the police for investigation and possible prosecution. In this process, the possibility of being caught may provide a deterrent against fraudulent multiple voting.[30]

Also, within the tech category, electronic poll books can facilitate the management of voter registration. These electronic lists substitute or supplement paper voter lists at voter identification tables at polling stations. Poll workers can look for the voter names or the voter's unique ID-number. Electronic poll books are used in 26.2 percent of U.S. jurisdictions, for example, to facilitate check-in and verification.[31] They can also be connected to a central server and allow voters to vote at the polling station of their choice, while controlling for voting multiple times. Their use has grown in the last decade, from primarily being utilized in North America and Europe to also include Latin America and parts of Africa. Recently, Kenya, Uganda and Ghana adopted their use, for example.[32] Technologies utilized for such systems can include desktop computers, fingerprint scanners, laptops, tablets, and sometimes proprietary mobile devices that are customized for the task. It should be noted that, as stated above, the devices can be connected to a network; however, this is oftentimes not the case and the devices operate standalone.

[30] Cookman, C. (2020). *Assessing Afghanistan's 2019 Presidential Election*. United States Institute of Peace. https://www.usip.org/sites/default/files/2020-08/pw_166-assessing_afghanistans_2019_presidential_election-pw.pdf

[31] National Conference of State Legislatures (NCSL). (2019, October 25). *Electronic Poll Books | e-Poll Books.* https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

[32] International Institute for Democracy and Electoral Assistance (International IDEA). (n.d.). *Is Technology Used for Identifying Voters at Polling Stations (Electronic Poll Books)?* https://www.idea.int/data-tools/question-view/740

Section III: Threat Actors and Their Motivations

Election infrastructure has been targeted by a variety of actors. These include states carrying out sophisticated operations, criminal groups, politically motivated actors, and insiders. As voter registration unfolds at the early stages of an electoral cycle, protecting voter PII and the tools and systems used for creating voter lists are early tests of an EMB's cyber capacities and safeguards. As outlined above, the voter registration system often has components that are accessible to the public online. In some contexts, the voter registration database is also utilized for other public services, which may also be exposed to the Internet. This accessibility makes voter registration databases and voter information an attractive target.

A. FOREIGN STATE ACTORS AND ADVANCED PERSISTENT THREATS

Malicious actors working within or affiliated with foreign states may have multiple reasons for targeting voter registration processes and associated voter data – from obtaining PII of citizens to undermining trust in an EMB and the elections it oversees or potentially to gather data about voters for targeted influence campaigns spreading disinformation.

Foreign Advanced Persistent Threats (APT), which can be defined as "an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives,"[33] have targeted voter registration systems. Before the 2018 parliamentary elections, Colombia's national voter registration web platform containing records for 35 million voters sustained over 50,000 attacks, according to government and military officials who attributed some of them to foreign state actors.[34] In 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation reported that an Iranian APT had scanned and attempted to access voter data in the U.S. from late September into October – successfully breaching cyber defenses in at least one state.[35]

Attribution of foreign attacks can be difficult and is generally denied by national governments. For instance, the government of Iran denied FBI allegations that it was behind an email campaign working to intimidate US voters in the 2020 elections. The Kremlin similarly denied that it had been attacking American electoral processes.[36] When a U.K. voter registration site crashed a little over two weeks before the 2016 Brexit vote, a Parliamentary Committee investigation explicitly did not rule out the possibility of a DDoS (distributed denial of service) attack using botnets originating from a foreign state.[37] Unfortunately, foreign

[33] NIST. (n.d.). *Glossary: Advance Persistent Threat.* https://csrc.nist.gov/glossary/term/advanced_persistent_threat

[34] O'Connor, S., Hanson, F., Curry, E., Beattie, T. (2020, October 28). *Cyber-enabled foreign interference in elections and referendums*. The Australian Strategic Policy Institute. https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

[35] United States Cybersecurity & Infrastructure Security Agency (CISA). (2020, October 30). *Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data*. https://www.cisa.gov/uscert/ncas/alerts/aa20-304a

[36] Collier, Kevin. (2020, October 21). Iran and Russia deny FBI accusation they are behind threatening emails sent to Florida Democrats. *NBC News.* https://www.nbcnews.com/tech/tech-news/fbi-says-iran-behind-threatening-emails-sent-florida-democrats-n1244228

[37] United Kingdom House of Commons Public Administration and Constitutional Affairs Committee. (2017, April 12). *Lessons Learned From The EU Referendum Twelfth Report of Session 2016-17.* (pp.102–03). https://publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/496.pdf

state actors and APTs may be particularly well-resourced and motivated to conduct attacks on voter registration to exert (or threaten to exert) influence on public trust.

B. GOVERNMENT ACTORS

Government actors may interfere with electoral processes in their own countries, particularly in autocracies, hybrid regimes, or democracies where government components are subject to weak institutional controls. They are generally motivated by a desire to secure an incumbent victory in an election. Disenfranchising or intimidating opposition voters using cyber operations works to this end. Alternately, they may use voter registration details that are not available to opposition actors to engage in targeted campaigning. It is widely believed that Zimbabwe's ruling party, ZANU-PF, gained access to millions of voters' mobile phone numbers from the voters' register and used it to target the electorate for its 2018 election campaign outreach.[38] Leading up to the 2013 general election in Zimbabwe, the ruling party also spread a rumor that the fingerprints collected during the country's first biometric voter registration drive in 2012 could be used by the Zimbabwe Electoral Commission (ZEC) to identify who citizens voted for by scanning the ballot papers. ZEC did very little to dispel this allegation as being false.[39]

To date, there is little documented evidence of exploitation of voter registration information systems' vulnerabilities by government actors to compromise confidentiality, integrity, or availability of the data. However, this lack of evidence may be due to governments' capacity to hide abuse of voter registration processes, rather than an absence of wrongdoing. Therefore, EMBs and their partners should not discount potential government interference into the VR system.

C. CRIMINAL GROUPS

Criminal groups may have financial incentives to target voter registration processes – particularly given that voter databases may be a rich source of PII, which can be sold for a fee.[40] Expensive equipment such as laptops and digital cameras used for voter registration could also be an attractive target for burglary (particularly if facilities where they are stored are not well protected, or if they are vulnerable during transfer). Nigeria's Independent National Electoral Commission (INEC) experienced such a theft leading up to the 2010 voter registration exercise.[41] Equipment can be resold on the local black market.

---

[38] For details, see https://qz.com/africa/1325485/zimbabwe-elections-whatsapp-sms-spam-data-privacy-concerns-for-mnangagwa-chimasa/

[39] National Democratic Institute and International Republican Institute Zimbabwe International Election Observation Mission. (2018, August 1). *Preliminary Statement.* (p.3). https://www.ndi.org/sites/default/files/8-1-18-ZIEOM%20Final%20Statement%20w%3A%20Delegation-cs.pdf

[40] There are reports that numerous country-wide databases are available online. Sometimes these allegations are incorrect, such as the supposed Georgian breach of voters.cec.gov.ge: European Platform for Democratic Elections. (2020, April 6). *Georgia Reported leak of voter data raises questions*. https://www.epde.org/en/news/details/reported-leak-of-voter-data-raises-questions.html; sometimes they are legitimate voter registration lists that were breached and posted online such as the United States' consolidated database of 107 million voters investigated in 2022: Ignoffo, Zachary. (2021, August 14). *Voter Records of 107 Million Americans is Sold on the Dark Web*. Privacy Affairs. https://www.privacyaffairs.com/hacked-voter-records/; see also: Winder, Davey. (2018, October 30). 81.5M Voter Records For Sale On Dark Web Ahead of Midterm Elections. *Forbes*. https://www.forbes.com/sites/daveywinder/2018/10/30/81-5m-voter-records-for-sale-on-dark-web-ahead-of-midterm-elections/?sh=47eac5a72a0c

[41] BBC News. (2020, December 9). *Nigeria voter registration kit stolen at airport*. https://www.bbc.com/news/world-africa-11958945; The election authority in Atlanta, Georgia, experienced computer theft machines containing

Criminals can also be hired by foreign entities to direct attacks against important infrastructure, such as election related information systems. Russia has utilized both criminals and politically motivated groups to carry out proxy attacks against various target countries.[42]

D. NON-STATE POLITICAL GROUPS AND HACKTIVISTS

Hacktivists (defined as hackers with explicit social or political motivations) and non-state political groups may target voter registration processes for various reasons. For example, to damage the credibility of an EMB, or to attempt to influence voter numbers to support a preferred party. In the Philippines, two hacktivist groups targeted the EMB to signal discontent with the overall electoral process and concerns about the security of electronic voting in 2016.[43]

An important caveat regarding hacktivists' and non-state actors' motivations for targeting election processes, and voter registration in particular, is that attribution can create confusion about who ultimately is behind a security breach, and why they carried out an attack. Specifically, hacktivists may use foreign IP addresses to mask their locations within the state, and in doing so, appear to be operating as a foreign actor. For example, in 2019 the voter registry database of Indonesia was targeted by a series of attacks originally attributed to Chinese and Russian actors. Ostensibly, these attacks were aimed at disrupting and discrediting the Indonesian voting process. The EMB's IT team later corrected initial statements, explaining that the attacks may have originated amongst local groups that were using foreign IP addresses to falsify their location.

E. INSIDER THREATS

Discussion of insider threat motives is largely speculative, given that undermining EMB systems and safeguards is likely covert and opaque. However, it is feasible that individual or collective threat actors could operate from within EMBs – as staff, consultants, contractors, volunteers, or trusted partners – to target voter registries for any number of reasons, including political leanings, personal grudges, or financial gain. For example, the FBI reported that a disgruntled former employee of a medical equipment packaging company utilized a "secret account on the company's computer system that he'd created before he was fired" to sabotage shipments of personal protective equipment in early 2020 as the COVID-19 pandemic unfolded.[44] This sort of abuse of access by employees and former employees can be hard to prevent and detect. Election officials can also be threatened or coerced to share access to sensitive databases. Shortly before election-day in Kenya in 2017, for example, the election commission's IT manager was tortured

---

the state's entire voter register in 2019. For details, see: Niesse, Mark. (2019 September 17). Check-in computer stolen in Atlanta hold statewide voter data. *The Atlanta Journal-Constitution*. https://www.ajc.com/news/state--regional-govt--politics/voter-registration-computers-stolen-from-atlanta-precinct/0W40RoNQQ3maPRUt3KPYnL/

[42] Russia has been reported to divert technically proficient criminals to work in cyber operations instead of prosecuting them. That strategy and other recruitment strategies are reported in: Kramer, Andrew E. (2016, Dec 29). How Russia Recruited Elite Hackers for Its Cyberwar. *The New York Times*. https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html

[43] Radware. (2016, March 28). *Philippines Election Commission Breach.* https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/comelec/

[44] United States Federal Bureau of Investigation. (2021 January 6). *Medical Equipment Packaging Company Hacker Sentenced.* https://www.fbi.gov/news/stories/hacker-who-disrupted-ppe-shipments-sentenced-010621

and murdered, allegedly in order to obtain passwords to the IEBC's sensitive databases.[45] Seemingly, the IT manager's statements prior to the incident that he would safeguard election related information systems from interference made him a target.[46] Where EMBs owns and maintain data centers that house significant computing resources, insiders can be motivated to utilize those resources for personal gain, for example by selling access or using computing resources to mine cryptocurrencies.

Section IV: Cybersecurity Risks Across the Voter Registration Process

Across the voter registration process, each step – from capturing voter information up until using it during an election – holds cybersecurity risk. This section provides a starting point to help readers understand some key risks. It is not, however, comprehensive. Risk should be considered within local context; each country must be evaluated in terms of the technologies used, available cybersecurity and governance capacity, and local social, political, and cultural factors.

A. CAPTURING VOTER INFORMATION

KEY RISKS:

- Physical devices: theft and tampering
- Using security good practices when connecting databases across networks for data exchange among other ministries, vendors, and third-parties

For voter registration processes using periodic or continuous voter lists, data is generally collected from citizens at the local level – and the physical security of the devices used to collect and transfer this data is a primary concern for an EMB. This decentralized nature of collection and consolidation means that a large number of devices are scattered through offices across the country, and the security of devices at each of these locations varies depending on the level of resourcing they receive, office configurations, and employees' training. Equipment theft, particularly laptops or USB drives, may occur.[47] While the crime may be qualified as a burglary, it often damages the reputation of the EMB, and raises suspicion from the public and political parties, who may question the EMB's management practices across other electoral processes and infrastructure as a result. It can also trigger investigations from police and data protection agencies.

[45] Omolo, K & Odhiambo, O. (2018). Chris Msando killed over a password, says Raila Odinga. *The Standard.* https://www.standardmedia.co.ke/entertainment/local-news/2001251941/chris-msando-killed-over-a-password-says-raila-odinga-as-slain-iebc-ict-manager-is-buried

[46] Ibid.

[47] USB drives containing voting machines' configuration files were stolen in a warehouse with lax security in Philadelphia in 2020, see: Bajak, F. & Lauer C. (2020, October 1). Laptop, USB drives stolen from Philly election-staging site. *Associated Press*. https://apnews.com/article/voting-machines-voting-custodio-elections-philadelphia-f8a6453dc9e211ef20e9412d003511b1

Cultural Variations in Data Sensitivity

The sensitivity and impact of data theft is highly dependent on culture and political context. For example, a leak of a small amount of biometric data about women in a traditional context can have a significant impact on the EMB's credibility and reputation and even have serious consequences for the women's reputations. Some countries record religion and ethnicity as part of the voter registration process because there are reserved seats in the national assembly where specific eligibility criteria have been set. For at-risk ethnic groups and other marginalized populations, information leaks can also threaten their safety, hence why the security and privacy of these lists are paramount. Some U.S. states keep voter information confidential for victims of domestic violence, sexual assault, stalking, and other crimes.[48] Other countries may consider that all the information on the voter list is public and have little to no restrictions placed on who can access it. Across all these contexts, impacts from unauthorized access or disclosure may vary greatly, from minimal in nature to seriously harmful.

Threat actors may also gain unauthorized access to voter lists. Devices can be physically compromised, although this requires physical access to the premises where they are used or stored. Remote access can be used to compromise devices that are connected to the Internet; the attack can be targeted at specific polling stations or constituencies, or to reach the whole electorate.

Transferring data or physical devices can risk the integrity and confidentiality of voter information. For instance, flash drives and hard drives managed by local authorities may be vulnerable to theft or tampering when loaded into vehicles going to central locations for voter list consolidation.

Finally, there are risks for countries relying on civil registries to create voter lists as well. Interconnecting or extracting data from these databases does not necessarily lower the cybersecurity risk involved in voter registration. The civil registration administration's security posture could be lower than the electoral authority's, and cybersecurity unfortunately tends toward a "lowest common denominator" of interconnected systems. Interconnecting different databases without appropriate controls could also create fresh vulnerabilities that could potentially affect both systems.

One central concern in cybersecurity is ensuring proper "segmentation" and "compartmentalization" between elements of interconnected information technology infrastructure when interconnection is necessary – ensuring that only required data and services are made accessible and only to the required systems and users. If this segmentation is insufficient, compromised technology in one connected institution could permit access of threat actors to EMB systems. To mitigate these risks, the institutions can sign a Memorandum of Understanding (MoU) specifying the requirements and responsibilities for security and the standards of each party.

If data or records will be extracted from civil registries, it is important to follow good cybersecurity practices to protect their movement between systems. This includes using tools that verify the integrity of information along with encrypted transfer mechanisms. When data will be physically transferred via

[48] National Conference of State Legislatures (NCSL). (2022, January 3). *Access To and Use of Voter Registration Lists.* https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx

media (e.g., hard drive, USB drives, and optical media), chain of custody documentation can help ensure the media is unaltered. However, it is important to note that interconnection may also introduce risks in contexts where civil registries may be controlled by incumbents or ruling parties. Such connections could allow those in power to interfere with voting processes or lead to perceptions of interference that call into question the ability of EMBs to independently manage the election process.

B. STORING AND PROCESSING VOTER INFORMATION

KEY RISKS:

- Database confidentiality and integrity
- Biometric data that can be leveraged for identity theft
- Public perception management around centrally storing personally identifiable information
- Ransomware and wiper[49] attacks against centralized data infrastructure

Once the voter information is centralized, several risks increase substantially. Adversaries do not need to infiltrate hundreds or thousands of devices to attack the voter registration list or steal data and equipment. Rather, they can target one central data center or system. The potential damage to the EMB's credibility and the integrity of the electoral process from data destruction or leakage rises exponentially given the sheer number of records that can be compromised in a single attack. There have been instances of nationwide database leaks in Mexico (where 93 million individuals' records were compromised)[50] and in the Philippines (where 55 million voter records, including biometric data were compromised).[51] In 2018, cybersecurity researchers reported a database was available for sale on a dark web hacking forum that contained data of more than 35 million voters from 19 U.S. states. The researchers determined that given the nature of the data they analyzed, the threat actor *"may have persistent access and/or contact with government officials from each state."*[52]

Databases containing biometric data may be particularly attractive targets. With access to individual biometric information, like digital photographs, threat actors can use the data for purposes beyond simple identity theft. Biometric data can be a particular concern in places where domestic government actors have access to facial recognition or other biometric data that was originally collected for VR but can then allow them to disenfranchise specific groups or individuals through enhanced surveillance. Some countries are using or considering the use of facial recognition technology to enable access to sensitive information, such as personal tax accounts, which would further increase the value of such data to criminal actors.[53]

Depending on the extent the VR process integrates such biometric information directly, or via interfacing with other government databases, it too could become an increasingly desirable target. Collection of biometric information may also heighten public perceptions of possible malfeasance, even if direct evidence of such activity has not been documented. For example, the use of fingerprints in Venezuela to

[49] A wiper attack refers to a cyberattack that makes data irrecoverable through deleting or "wiping" the data.

[50] Galvàn, Melissa. (2018, October 7). El INE denuncia la venta en internet de una copia de la lista de electors. Expansiòn Política. https://politica.expansion.mx/mexico/2018/10/07/el-ine-denuncia-la-venta-en-internet-de-una-copia-de-la-lista-de-electores

[51] Temperton, James. (2016, April 14). The Philippines election hack is 'freaking huge'. *Wired*. https://www.wired.co.uk/article/philippines-data-breach-fingerprint-data

[52] Anomali Threat Research. (2018, October 15). *Estimated 35 Million Voter Records For Sale on Popular Hacking Forum.* Anomali. https://www.anomali.com/blog/estimated-35-million-voter-records-for-sale-on-popular-hacking-forum

[53] Internal Revenue Service. (2022, February 7). *IRS announces transition away from use of third-party verification involving facial recognition.* https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition; see also: United States Government Accountability Office. (2021, April 24). *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*. https://www.gao.gov/products/gao-21-526

authenticate voters and activate electronic ballots has been accompanied by widespread public fear that they could allow the government to compromise the secrecy of their vote and target them for some form of retribution.[54]

Manipulation of voter lists, disenfranchisement of targeted groups of voters, and any other alteration of voter records become possible at scale at this phase of data consolidation. In the U.S. for example, reports emerged in 2019 of intrusion by Russian government affiliated groups into voter registration systems used in the 2016 elections. While nearly all states' electoral systems were probed to find vulnerabilities, only a small number were compromised; investigators reported that foreign actors were *"in a position"* to alter the voter registry data.[55]

A more common problem, as evidenced in the U.S. case, is the improper purge of voter registers by election authorities. In some instances, hundreds of thousands of voters have been deleted from voter lists because of error-ridden practices and the affected voters were not properly informed.[56] Thoughtful transparency, such as through automated notifications to individuals being removed from voter lists or when other changes to their voter registration are made, can help minimize the impact and remove incentives for manipulation in the first place.

Remotely activated malware could erase the voter database on a network-connected server. Even in the case of a data center or central database that is not connected to the Internet, there are classes of malware that are specifically designed to reach 'air-gapped' infrastructure, which are systems that are not connected to a network accessible via the Internet, to inflict damage.[57] Financially motivated actors usually do not target EMBs, given their known limited capacity to pay. This may reduce the likelihood of ransomware attacks on them that some other government institutions are targets of, as Costa Rica's financial and health ministries has experienced.[58] But the risk should not be excluded completely, as foreign state actors and APTs might use criminal groups as proxies to complicate attribution and maintain plausible deniability. Whatever the motivation or actor, a spectacular wiping of a voter list central database would require the EMB to undertake major efforts to recover the data from backups (if any) or go back to the devices used to collect the information in the first place (if possible). Such disruptions during critical election windows can have significant impacts on electoral integrity, even if recovery is possible within a relatively short period of time.

Risks to physical infrastructure should not be neglected either. The centralization of one data center or system makes for an attractive target for adversaries. Some EMBs co-locate their infrastructure with other government data centers. While this has benefits in terms of security and cost, many election authorities

[54] Rueda, Jorge. (2012, August 6). *Thumbprint readers stir fears in Venezuela Vote*. Yahoo!Finance. https://finance.yahoo.com/news/thumbprint-readers-stir-fears-venezuela-vote-131434477.html

[55] Robles, Frances. (2019, April 26). Russian Hackers Were 'In a Position' to Alter Florida Voter Rolls, Rubio Confirms. *The New York Times.* https://www.nytimes.com/2019/04/26/us/florida-russia-hacking-election.html

[56] Morris, K. & Pérez, M. (2018, July 20). *Purges: A Growing Threat to the Right to Vote.* Brennan Center For Justice. (p.1). https://www.brennancenter.org/our-work/research-reports/purges-growing-threat-right-vote

[57] The Stuxnet malware discovered in 2010 specifically designed to target information and controls systems of the Iranian Nuclear Program remains the most striking example of an air-gapped virus. See Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon.* Broadway books.; A recent study from E-Set shows that air-gapped attacks have grown in sophistication and frequency: Dorais-Joncas, A. & Munõz, F. (2021 December). *Jumping The Air Gap: 15 years of nation-state effort.* ESET. https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

[58] Rosch, Carla. (2022, June 1). *A massive cyberattack in Costa Rica leaves citizens hurting.* Rest of World. https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/

worry about the impact on and perceptions of their independence and prefer to deploy high-cost technologies that may not be sustainable.

Finally, as mentioned earlier, powerful processing servers used for biometric voter registration (BVR) matching could be a particularly attractive target for adversaries to use to mine cryptocurrencies,[59] an operation that requires heavy computing and reaps financial rewards. For the EMB, co-option of BVR servers for such purposes would considerably slow down the matching process, prevent on-time delivery of reliable voter lists, and even disrupt or delay an election by interfering with voter matching. This type of attack has not yet been reported in the voter registration context, to the authors' knowledge, but it is a real risk for biometric servers.[60]

C. USING VOTER INFORMATION DURING THE ELECTORAL PROCESS

KEY RISKS:

- Risks to availability such as denial of service attacks that make EMB infrastructure unavailable during key electoral periods
- Supply chain risks, such as compromised vendors
- Poor voter list verification services that allow undue access to voter information
- Disinformation that confuses and misinforms voters

When technology is used in polling stations, EMBs need to consider how malign actors may attack or spread disinformation about these technologies to disrupt, manipulate, or undermine the electoral process. Electronic poll books, whether used as standalone devices or integrated into biometric voter identification or electronic voting machines, can be targeted by DDoS attacks. This would potentially impact the ability of the EMB to prevent people from voting multiple times and to efficiently process voters. Where electronic poll books become unusable, the absence of physical copies of voter lists at each polling station could disenfranchise groups of voters unable to travel to their original polling station who were relying on the networked nature of electronic poll books to verify their ability to vote, even if not at their normally assigned location.

Any device deployed in the polling station, including electronic poll books and electronic voting machines integrating voter registration data, needs to be protected throughout its lifecycle. Devices can be compromised individually or in bulk by targeting the vendor, as well as during transportation and storage on EMB premises. This applies before and after they are used at the polling stations if the equipment will be re-used during several election cycles. Electronic poll books might be compromised by third-party vendors or suppliers to selectively disenfranchise specific voters during an election based on their age, gender, or any other criteria that can be identified by the machine. Devices can also be misused by operators if they find vulnerabilities that allow them to manipulate the voter identification process without being detected.

Providing online services to voters to access and update their personal information increases cybersecurity risks, as these services require a database be connected to the internet. Good practice entails maintaining one database that interacts with voters and another "master" database that is updated after changes are audited. However, even breaches that are found and inaccuracies or manipulated data that is corrected

[59] In cryptocurrency networks, *mining* is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating an incentive to carry out the validation task, which is increasingly complex as the transaction ledger grows. See Grabowski, Mark. (2019). *Cryptocurrencies: A Primer on Digital Money*. (pp. 7-18). Routledge.

[60] Heinemeyer, Max. (2020, September 20). *How AI caught hackers crypto-mining on a biometric access server in an empty office.* DarkTrace. https://www.darktrace.com/en/blog/how-ai-caught-hackers-crypto-mining-on-a-biometric-access-server-in-an-empty-office/

can disrupt and cast doubt over an EMB's capacity to conduct an election. Preserving the balance between accessibility (providing more services to users to improve voter turnout) and privacy (see the callout in section II) remains a challenge for many EMBs.

Poorly protected voter registry verification services can allow malicious actors to intercept or scrape content from the voter registry, in whole or in part. For example, if individual voter records can be accessed online without proper login or using easily guessed default passwords that are infrequently changed by newly registered voters, automated scripts running for a few days can collect vast numbers of voter records, one by one, by simulated human interaction through the voter registration website.[61]

The voter-oriented services operated by EMBs, and their contracted vendors, can also be manipulated to spread confusion by distributing incorrect information during the election, like providing voters wrong polling location information when they consult the portal. There have been instances where systems are found to be sending fake SMS messages in bulk while spoofing (imitating) the EMB caller ID to distribute disinformation, such as in Kenya in 2017.[62] EMBs often use a variety of external communication methods, but even if one or two of them are subverted, the effects can be significant.

The risk of disinformation is beyond the scope of this briefing paper. However, disinformation campaigns can exacerbate concerns about EMB performance and the accuracy of voter lists, which can exacerbate the damages from cyber-attacks. In Indonesia, for instance, news about the EMB's removal of foreign nationals from a voter list fueled public concern about foreign laborers voting in state elections in 2019.[63]

Section V: Potential Types of Attacks

Cyber-attacks target vulnerabilities in software and hardware, user behavior, and gaps in policy and procedures that can be exploited to compromise the confidentiality, integrity, or availability of information in electronic systems. Cyber threat actors make use of many different tactics, techniques, and procedures (TTPs) to achieve their goals.[64] TTPs are important to consider since certain variations of techniques, tactics, and procedures can help distinguish one threat actor from another. Discussion of cybersecurity TTPs could easily extend into granular technical dimensions, but this paper will only provide an introduction of how various threat actors employ and favor specific *methods, tools,* and *actions*.[65]

At each stage of the voter registration process, the information technology infrastructure can be exploited through a variety of techniques and tactics. Often threat actors can exploit improperly configured servers or datasets exposed on the Internet. Such misconfigurations are the most common enabler of the breaches

---

[61] Web-scraping is a technique used to extract data from websites and online sources. It can be done manually but is usually automated using specialized software such as bots or web crawlers that emulate human browsing of data and collect it in bulk.

[62] Purdon, Lucy. (2018). A Very Secret Ballot. *SUR-Int'l Journal. on Human Rights. 27*, 91. https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-lucy-purdon.pdf

[63] Lamb, Kate. (2019, March 19). Indonesia election mired in claims of foreign hacking and 'ghost' voters. *The Guardian.* https://www.theguardian.com/world/2019/mar/19/indonesia-election-mired-in-claims-of-foreign-hacking-and-ghost-voters

[64] NIST. (n.d.). *Glossary: tactics, techniques, and procedures.* https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures

[65] For a comprehensive discussion of TTPs that maps selected tactics, techniques, and procedures to specific tools and methods for specific threat actors, see the MITRE ATT&CK framework available here: MITRE. (n.d.). Att&ck. https://attack.mitre.org/

of voter information that have occurred over the last years. With more EMBs turning to third-party solutions that may not be implemented using experienced and qualified professionals, unprotected or poorly protected databases are a high risk. Additionally, insiders can facilitate access to the data to criminal groups.[66] The following table highlights some of the most utilized tactics and techniques that can lead to compromised voter registration infrastructure.

COMMON TACTICS, TECHNIQUES, AND PROCEDURES	
PHISHING	Tricking users to disclose sensitive information, such as usernames and passwords, or to allow malicious software to be downloaded and deployed. This is often done by sending out emails or other communications (such as text messages or via other messaging applications) asking recipients to click on malicious links or respond with sensitive information.[67]
SPEAR PHISHING	A far more targeted variant of the phishing technique. Often states and sophisticated actors will tailor the content or presentation of messages to make it more likely the target will be tricked, based on intelligence and specific information about that individual or entity. Threat actors may also target vendors that have privileged account access to perform essential business functions and use that access to pivot to target the main entity's systems. For an EMB, voting technology vendors, logistics providers, and third-party service providers should all be considered partners that hold themselves to having robust cybersecurity.
INTERCEPTION AND COMPROMISE OF PHYSICAL DEVICES	A tactic that is frequently encountered in voter registration processes when devices are in transit. Stealing devices for their monetary value – or the potential value of the data they hold – is common. Laptops or hard drives and PII can be easily resold on the black market or dark web. Relevant examples of theft have been reported in Hong Kong[68], the Philippines[69], Malawi[70], Canada[71], and the U.S. (Atlanta).[72] Access to the physical devices where the data is stored may allow malicious actors to manipulate the list, adding names either manually or via automation. Specially crafted malware can be developed and injected via USB, allowing for further manipulation. Access to the voter registration machines, even for a few seconds, can compromise the integrity of the list. In the most extreme cases, if the disruption of the election operation is the ultimate objective, actors might choose to simply destroy the devices and/or their contents.

Table Continued on Next Page

[66] In 2020, the distribution of an official PDF from the Indonesian KPU was distributed by a criminal group online. The full investigation was not published, but it was alleged that the criminals were the recipient of an internal leak, https://en.tempo.co/read/1345108/kpu-alleged-hacking-leaves-2-3-million-personal-data-compromised

[67] Robles (2019)

[68] Ng, Yi Shu. (2017, March 28). *The personal data of all of Hong Kong's 3.7 million registered voters have been stolen.* Mashable. https://mashable.com/article/hong-kong-voter-data-stolen

[69] Bueza, Michael. (2017, February 20). *Confirmed: Comelec computer stolen in Lanao contains national voters' list.* Rappeler. https://r3.rappler.com/nation/162016-national-voters-list-stolen-comelec-computer-wao-lanao-del-sur

[70] Sangala, Tom. (2018, October 20). *Voter registration 'kit' stolen.* The Times Group. https://times.mw/voter-registration-kit-stolen/

[71] CBC. (2012, June 5). *Elections NB doubts voter data targeted by laptop thief*. https://www.cbc.ca/news/canada/new-brunswick/elections-nb-doubts-voter-data-targeted-by-laptop-thief-1.1134711

[72] Daugherty, Owen. (2019, September 17). *Two computers stolen from Atlanta polling site contain statewide voter data.* The Hil. https://thehill.com/homenews/state-watch/461872-two-computers-stolen-from-atlanta-polling-site-contain-statewide-voter

TARGETED BOTNET OPERATIONS	Botnets are collections of Internet-connected computers that have been compromised and are under the coordinated control of a malicious threat actor. Often criminals will rent their command-and-control infrastructure for targeted attacks against specific websites and online entities. The resulting (DDoS) attack results in a loss of availability, as targeted websites become overloaded with requests and are inoperable.[73]
WATER HOLING	This type of attack uses fake websites that may emulate a legitimate website or seem to serve a legitimate purpose but are in fact allowing malicious actors to exploit users. Sometimes attackers set up websites that look similar or identical to legitimate companies' or governments' websites.
PASSWORD SPRAYING	This very common type of attack relies on the fact that many people use the same password across accounts. If a threat actor has compromised a personal account of a person who works for the EMB, they can try and use the same password across other accounts associated with that individual in hopes the individual used it in their professional life too.
SUPPLY CHAIN ATTACKS	Supply chain attacks compromise hardware and software components prior to the point of use (e.g., inserting a hardware modification or software vulnerabilities during or after the manufacturing or software engineering process but before the product has been integrated into an EMB's IT infrastructure). The recent breach of software company Solar Winds is an example of this type of attack.[74] Supply chain considerations also include identifying and vetting trusted providers to ensure their transparency and that their products do not incorporate untrusted or compromised components.
SOCIAL ENGINEERING	Often relies on means that are not technological, but rather exploit human nature to gain sensitive information that can be used to compromise electronic systems. Examples include criminals posing as customer service representatives over the phone and tricking targets into disclosing sensitive passwords and PIN numbers.
MAN IN THE MIDDLE	Consists of intercepting communications between users and a legitimate destination to read or change the communication before relaying the information onto the destination, without having compromised the destination website or system. Electronic poll books or other network-connected devices can have their communication intercepted by devices used near or at the polling. Devices that use wireless connections that are not well encrypted are particularly at risk.
RANSOMWARE	Often the techniques discussed above are leveraged to compromise networks to deploy software that encrypts the data on target systems in a type of attack termed "ransomware." Threat actors may then contact the victim and offer to decrypt their data for a fee. Such a tactic can also be used for destructive attacks that cause deletion of information or other negative effects.

[73] For an example, see the various DDoS attacks against the Ukrainian Central Election Commission detailed in: Martin-Rozumilowicz, B. and Chanussot, T. (2019 October). *Cybersecurity and Electoral Integrity: The Case of Ukraine*, 2014-present. In Krimmer, R., Volkamer, M., Beckert, B., Driza Maurer, A., & Serdült, U. Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019: 1-4 October 2019. (278-292). Lochau/Bregenz, Austria: Proceedings. https://www.zora.uzh.ch/id/eprint/175950/1/Krimmer_et_al_E-Vote-ID_2019.pdf

[74] A threat actor compromised Solar Winds' software update process, and since Solar Winds software was used widely by other companies and entities to monitor their networks, threat actors were then able to compromise these other networks. For background on the Solar Winds breach, see United States Cybersecurity & Infrastructure Security Agency. (n.d.). *Supply Chain Compromise*. https://www.cisa.gov/supply-chain-compromise

Section VI: EMB Approaches to Securing Voter Registration Processes

There are several strategies that EMBs can use to mitigate risks to voter registration processes. They include protecting the physical tools used for data capture and transfer, the databases and the PII of voters they house, and the security of preliminary and final voter lists. Vulnerabilities will vary depending on how an EMB creates voter lists – that is, whether it's done using a periodic list, continuous registry, or civil registry model of voter registration.

Regardless of which approach is used, EMBs and other stakeholders can draw on risk management and security control frameworks that are considered good practice in cybersecurity. These frameworks offer approaches to inventory electronic information devices and the sensitive data they hold; assess the risks to these assets, along with strengths and weaknesses in their current cyber defenses and capacities; and then prioritize mitigation efforts.[75] Some overarching security considerations include ensuring that EMB staff and others play a role in protecting the integrity of voter registration processes – including third party vendors – with clear guidance and the required skills to prevent and respond to cyberattacks. Specific action items may include:

- Carefully vetting potential bidders during tender processes to identify security risks.
- Providing clear, formalized security requirements to third party vendors providing devices used for voter registration and verification, and services required for the maintenance of databases.
- Introducing controls against common types of attacks such as phishing and spear-phishing (e.g., by providing EMB staff and data clerks responsible for voter registration with training and resources on these common types of attacks, how to identify them, and how to report them), and for DDoS attacks through services that can help recognize and filter legitimate traffic and requests from illegitimate traffic and requests meant to overwhelm, slow, or interrupt services.

The remainder of this section briefly outlines challenges and tasks that EMBs may face in their efforts to securely capture, transfer and store, and use voter registration data and produce accurate voter lists. It also presents generally applicable steps to reduce risk at each stage of the registration process.

A. CAPTURING VOTER INFORMATION

Devices and tools used for data capture need to be secured, whether they are electronic (e.g., laptops and tablets) or physical (e.g., paper forms). Key steps that can be taken to mitigate risk include:

- Ensuring the physical security of the end-point used for the voter registration (dedicated hardware or personal computer). Consider: locked doors/storages, window bars, tamper evident seals.
- Ensuring the software security of the end-point is equally important. Laptops should automatically lock after inactivity, and connected devices should be protected by firewalls and other network protections. Software and operating systems should be maintained up to date with the latest available security patches. End point protection or advanced antivirus software should be installed and up to date. Importantly, unlicensed, pirated, or second-hand software, including operating

[75] For further information regarding security controls and risk management frameworks, see *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document.* The standard frameworks applicable to this process include: NIST SP 800-37. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf in conjunction with NIST SP 800-53. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final; The European Union's Agency for Cybersecurity also publishes a Risk Management/ Risk Assessment Framework for cybersecurity. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework

systems, should not be used on any system that connects with elections infrastructure because it is often accompanied by malware and generally cannot be patched, leaving systems vulnerable.
- Data should be encrypted while stored on devices, and also when copied to other media (onto a USB stick, portable hard drive, or when transmitted to another location).
- Good access control practices should be enforced with strong password protection and multifactor authentication. Some BVR kits allow operators to authenticate using their fingerprints, which should not be substituted for multifactor authentication.
- Authentication and modification of the data should be recorded on the device, and those records should be protected from alteration, to provide traceability for all activities.
- There should be appropriate backup procedures in place. They should be tested and, if possible, automated, to safeguard against theft or physical failure of the device. Ideally backups should be automated and backup data should be maintained at a separate location (online or at a separate data center) to ensure that physical emergencies such as fires or floods do not destroy both the backup and primary copies of the data.

B. STORING AND PROCESSING VOTER INFORMATION

When data and devices are in transit – whether electronically or physically – security measures must be taken. EMBs may consider:

- Enforcing physical protection of the devices used for the data transfer – for instance, using sealed, tamper-evident envelopes for transport, or providing police escort for devices.
- Encrypting all data on devices used for transportation (for example, when using USB media like small thumb drives)
- Using dedicated network lines or enforcing hardware-based VPN connectivity using modern encryption standards for telecommunications.

Servers on which voter data is stored also require security measures, such as:

- Segregating biometric data and PII from other data, potentially in separate databases. All databases should be encrypted according to industry standards.
- Maintaining logs that record authentication, modification, and access to voter data to provide traceability for all activities. These logs should be protected from unauthorized access and tampering.
- For physical servers, setting up security measures such as closed-circuit television, biometric or two-factor locks, movement detection alarms to prevent tampering, and possibly stationing guards to protect physical assets.
- For remote servers, using anti-virus protections, as well as maintaining software and operating systems and installing available security patches on a timely basis.
- Undertaking continuous monitoring to detect equipment failure.
- Engaging in continuity and contingency planning in case servers fail, are damaged, or need to be shut down. As resources allow, EMBs may consider setting up secondary data centers for critical systems.

Additional activities can support the overall integrity of voter lists, including:

- Auditing changes to data logs and monitoring for anomalies in data entry – such as mass injections of data from a single systems user in unrealistically short periods of time.
- Undertaking comparative analyses to identify anomalous shifts in voter registration patterns –

using census data or voter lists from previous elections as a baseline, for instance, to identify major increases or decreases in registrant numbers in certain geographic areas.

C. USING VOTER INFORMATION DURING THE ELECTORAL PROCESS

A primary challenge in maintaining the security of voter lists and data in the lead up to election-day, and during polling itself, is protecting online databases and portals where this information is stored. EMBs and their partners can:

- Ensure that voter lists are available on a "read only" basis upon publication of preliminary voter lists (when parties, candidates and voters will have an opening to review, verify, update or challenge registration details) and final voter lists.
- Protect remote servers where voter information is stored through use of firewalls, vulnerability scanners, intrusion prevention systems, and intrusion detection systems (amongst other tools).
- Protect network-connected devices against DDoS.
- Consider continuity planning procedures, with failover to a secondary data center if critical systems are taken down.
- Protect against scraping by asking for a combination of personal data, using throttling and IP limits on the log-in page to limit vulnerability to automated collection methods.
- Well ahead of the election, conduct security audits to identify external and internal vulnerabilities; reserve time and funding to address and mitigate identified vulnerabilities.
- Collaborate with other agencies, including cyber security bodies, to coordinate incident response.

In the immediate prelude to elections, EMBs will need to take steps to secure voter lists and devices as they are transferred to and used at polling stations. EMBs may:

- Establish a chain of custody to protect the integrity of the devices during transportation and storage.
- Maintain physical paper-based backup copies of the voter list in case of unavailability or loss of integrity.
- Set up authentication and modification safeguards, to prevent and/or record changes to voter data.

On election-day, polling station workers will need to maintain situational awareness and act to protect voter lists, devices, or other tools used for voter verification onsite. EMBs may impart instructions through training and written guidelines about expectations and procedures for maintaining security.

Section VII: Programming Recommendations and Key Considerations

Citizens' right to choose their representatives and participate in their country's decision making through elections is the cornerstone of democracy. However, to be credible and to earn the public's trust, elections must be inclusive, accountable, transparent, and allow for genuine political competition. They also must be secure. Election cybersecurity – and the ability of election authorities to prevent and mitigate attacks on critical election processes, including voter registration - is therefore an important element of democratic resilience and a critical development challenge. To meet that challenge, USAID Missions and their partners and stakeholders can "…design and procure activities with the goal of improving

cybersecurity and cyber resilience…"[76] Such support is complementary to other forms of technical assistance, enabling USAID partners to promote credible election processes while also preventing cybersecurity breaches.

USAID Missions, other development agencies, and implementing partners can support stakeholders with a range of programs to help facilitate and maintain cybersecurity across the three main elements of the voter registration process – capturing, storing, and using voter information. The strategy outlined in the *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming* can be used as a guide. However, as stated previously, each country "…has its own unique digital ecosystem, which means cyber vulnerabilities and threats vary greatly depending on context."[77]

USAID and other development agencies can:

- **Support the development and implementation of cybersecurity assessments based on global best practice and as outlined above within this briefing.** The first step in addressing cybersecurity when supporting voter registration programming is understanding the cybersecurity capacity, capabilities, and related information technology context of the country and region. With that information, USAID and other development agencies can, in collaboration with EMBs and other stakeholders, systematically identify and prioritize vulnerabilities within the voter registration process that require the greatest attention.

- **Support relevant stakeholders, including EMBs and state legislators, to integrate good cyber practices into the voter registration process.** For example, this could include establishing policies and regulations concerning the storage and transmission of voter registration data to include minimum encryption standards, physical and electronic security standards, along with limits to what sort of information can be aggregated and stored concurrently in databases.

- **Support EMBs in strategic planning that integrates a life-cycle approach to technology implementation and sustainability.** Regulations, policies, and procedures should consider the entire life cycle of technology from initial requirement scoping through implementation, operation, sustainment and upgrading, and finally de-commissioning and disposal. Doing so will ensure security risks that emerge due to out-of-date or unmaintained technology are accounted for and minimized. USAID and other development agencies can help EMBs integrate such approaches into their strategic planning by providing expert consultation and technical assistance during planning phases.

- **Support the development of communities of practice or fund networking opportunities for key EMB information technology personnel to interface with other EMBs in the region or globally.** This could include programming that helps countries engage in good practice development for specific voter registration processes and workflows by drawing on input and experiences from other regional EMBs or internationally accepted practices of other EMBs across the globe. These networks and communities of practice could facilitate knowledge-sharing and lessons learned, especially as new technology, software, and cyberthreats emerge in the election space.

[76] USAID. October 2021. *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.* https://www.usaid.gov/sites/default/files/documents/USAID_Cybersecurity_Primer.pdf

[77] Ibid.

- **Assist EMBs in cost-effective and transparent procurement and investment of secure voter registration technology and infrastructure.** For example, the voter registration process may increasingly use "cloud services" to store and process voter information. To the extent that third-party service providers are employed, EMBs can be supported with technical assistance to ensure that chosen vendors adhere to security and transparency good practices. USAID can support activities that help EMBs and decision makers assess the reputability of private sector partners and facilitate the establishment of mechanisms for information sharing among trusted regional and global partners.

- **Promote and support training and technical assistance to build cybersecurity capacity among EMB staff and other stakeholders.** At each stage of the voter registration process, there are multiple constituencies, including government officials, EMB staff members, and others responsible for implementation of voter registration steps. Through training, technical assistance, and capacity building for both general cybersecurity practices and secure voter registration processes, the involved parties will be better equipped to adopt and implement proper cybersecurity procedures throughout every step. The introduction of a basic cyber hygiene training focused on individuals with access to sensitive data, such as staff at voter registration processing and intake centers, can help prevent techniques such as phishing as users are prepared to recognize and mitigate them. Further technical assistance tailored to the specific voter registration process of a particular EMB would build on the basic cyber hygiene training to provide EMB staff and other stakeholders tools to continue to adapt and strengthen their cybersecurity practices as technology and cyber threats evolve. Existing EMB IT and cybersecurity personnel can also benefit from technical training to improve and build necessary cybersecurity capacities such as designing security information networks, incident response forensic analysis, programmatic support, and cybersecurity auditing and technical testing.

- **Facilitate executive level training to help build cybersecurity managerial skills among government officials.** Exposing executive leadership to cybersecurity management skills can arm them with knowledge to support establishing and sustaining robust cybersecurity risk management programs and policies. With sound understanding of cybersecurity threats and approaches, EMB executives can be empowered to make resource decisions that integrate security holistically across the election process.