USAID
FROM THE AMERICAN PEOPLE

BALLOT PRINTING MACHINES
CONGO ELECTIONS IN 2018
AP PHOTO/JEROME DELAY

Briefing Paper: Cybersecurity of Election Results Management Systems

OCTOBER 2022

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

Acknowledgments

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). Ronan McDermott, Veronika Prochko, and Dr. Tarun Chaudhary were the lead authors. The paper benefited tremendously from contributions by Matthew Bailey, Erica Shein, 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

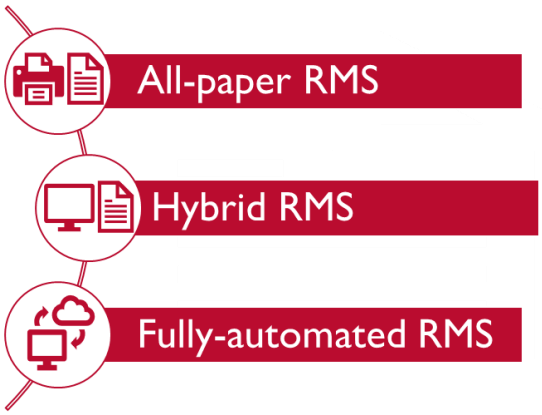
CONTENTS

Section I: Introduction

The famous phrase "it's not who votes that counts, it's who counts the votes"[1] highlights how crucial election results management is in the overall electoral process. Even citizens who have no interest in politics pay attention to the results management process – because everyone wants to know who won. Increasingly, in the age of rapid news cycles and social media, voters want results in real time – this puts additional pressure on already stretched elections management bodies (EMBs) and poll workers.

Nearly everyone would agree that the integrity of an election is greatly affected by how the results are managed. While *any* weakness in the entire electoral cycle can be exploited by those looking to overturn the will of the people, results management is carried out when the political temperature is highest and when the maximum scrutiny is placed on EMBs. Even the slightest anomaly or hiccup in results management can quickly snowball into a major political crisis – or worse, precipitate electoral violence.

Election results management starts once the votes are counted (most commonly at polling stations, but also at counting centers). Depending on the size of the country and the nature of the election (or elections, as many countries undertake multiple elections on a single day), results management will be more or less centralized. In many countries, the process is largely paper-based – particularly at polling stations – in the early stages. Varying degrees of technology are often used during the process. In many countries, technology reaches all the way into the polling station. No matter the presence or level of technology, the results need to be captured and stored, transmitted (or physically moved in low-tech settings), processed, and published.



The Results Management System (hereafter RMS) is the term used to describe the sum of these processes, and they are usually categorized as all-paper, hybrid, or fully-automated processes. RMS have slightly different security requirements compared to other electoral information systems. Since results data is typically in the public domain soon after being recorded on a paper results protocol form and shared with political party/candidate agents and citizen election observers, the emphasis is less on the ultimate confidentiality, and more appropriately on integrity and availability.[2] Given the intensely political nature of RMS, the entry points at different stages in the

[1] While no one knows who coined this phrase, it is frequently attributed to Josef Stalin, William "Boss" Tweed and Napoleon.

[2] In this context, "availability" refers not only to the protection of RMS from, for example, denial of service attacks, but also to the rapidity with which results data are made available for public dissemination by the EMB. "Integrity" refers to the uprightness and validity of the results, such that they remain free from interference and manipulation and "confidentiality" refers to having positive control of any electronic information involved during the results management process, ensuring results are released is in accordance with the plan and procedures set by election managers.

results management process and the fact that they are less protected and more accessible compared to most other parts of the election process make them an attractive target for malicious actors.[3]

Historically, counting ballots at polling stations was a way to prevent the government, either through the police or military, from taking ballot boxes off to remote (and inaccessible) count centers where, at their leisure, and away from public scrutiny, they could ensure their desired outcome. When vote counting at polls became the norm, paper results forms became the next target for manipulation. Tampering with forms on their way from the polling stations to constituency or district election offices became problematic. Tamper-evident envelopes or bags, sharing copies of the results forms with political party and candidate agents and citizen observers, and posting results forms outside the polling station all proved to be necessary improvements in the results management. Now, with digital technology well entrenched in the RMS process, equivalents to these "analog" paper-based integrity mechanisms, such as encryption, access controls, system logs, and integrity checks, have emerged.

Most recently, the use of parallel channels (frequently – though not always – a mix of paper and electronic) has been introduced to keep all players honest. Typically, technology is introduced which allows data from scanned paper-based results forms to be captured for storing and transmitting to the higher-level EMB. This provides both rapidly-delivered preliminary electronic data (for early results reporting) and a parallel, paper-based channel for validating results that arrive more slowly. In some countries, this data capture happens at constituency/district-level offices; in others, it takes place at a single national results center. In many countries, technology is deployed at the polling station level. This multi-level distribution of information technology presents enormous cybersecurity challenges.

This briefing paper was developed for the United States Agency for International Development's (USAID) Democracy, Human Rights, and Governance Center (DRG Center) to inform a broad audience, including USAID DRG personnel, USAID implementing partners, and local electoral stakeholders, on election results management systems and cybersecurity issues. Section II provides an overview of the RMS process and the key technologies often utilized. Section III examines RMS cybersecurity threat actors and their motivations. Sections IV and V examine cybersecurity risks and types of attacks on results management systems, respectively. Section VI examines options for elections management bodies to secure results management systems. Section VII includes recommendations for those tasked with programming technical assistance.

This briefing paper may be read in conjunction with the other products prepared by IFES' Center for Applied Research & Learning as a part of DAI's Digital Frontiers initiative in consultation with USAID's DRG Center, including *Primer: Cybersecurity and Elections*,[4] *Understanding Cybersecurity throughout the Electoral Process: A Reference Document*,[5] and *Briefing Paper: Cybersecurity and Voter Registration*.[6]

[3] Amoah, M. (2020, January). *Sleight is right: Cyber control as a new battleground for African elections*. African Affairs, *119*(474). (pp. 68–89). https://doi.org/10.1093/afraf/adz023

[4] Available electronically: https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf

[5] Available electronically: https://pdf.usaid.gov/pdf_docs/PA00ZK5H.pdf

[6] Available electronically: https://pdf.usaid.gov/pdf_docs/PA00ZK6G.pdf

Section II: Overview of election results management and the key types of technologies and data associated with each step of the process

Overview

The three basic models of results management systems are all-paper, hybrid, and fully automated. Electoral legal frameworks tend to vary widely with respect to using paper and/or technology in RMS. This leads to a high level of diversity (and therefore complexity) in what would seem to be a conceptually straightforward activity – the adding up of numbers of votes cast for a party, candidate or referendum choice.

RESULTS MANAGEMENT SYSTEMS, OR RMS

As defined by the United Nations:

A *"results management system (RMS) contains all elements related to the count, aggregation, analysis and publication of votes once they have been counted at the lowest level."*[7]

RMS may include three standard stages: (1) Capture and Storage of Election Results; (2) Transmission of Election Results; and (3) Processing and Publishing of Election Results.

An all-paper RMS uses paper-based forms at every level, completed first by the presiding officer (the most senior poll worker at a polling station or precinct,) and next by EMB officials at one or more levels of consolidation (i.e., wards, counties, districts, provinces, regions, nationwide). Generally, smaller countries have fewer levels of consolidation, while larger countries have more. India, for example, has five levels of consolidation.

A hybrid RMS is by far the most common. A hybrid RMS introduces technology somewhere in the process. At the simplest level, and often with no legal or procedural basis, an EMB official might use a calculator or simple computer-based spreadsheet to help tally results from multiple polling stations. Technology is used here as a tool to enhance accuracy and speed up the process, as there is always pressure in an election to deliver rapid results. In an increasing number of countries, hybrid RMS means that technology is deployed at the polling station level, where staff capture information from the results form for storage, transmission, and subsequent processing. In a hybrid RMS, understanding which results (paper or digital) are legally binding is critical, as well as knowing when one form of results is legitimate if the other has been compromised.

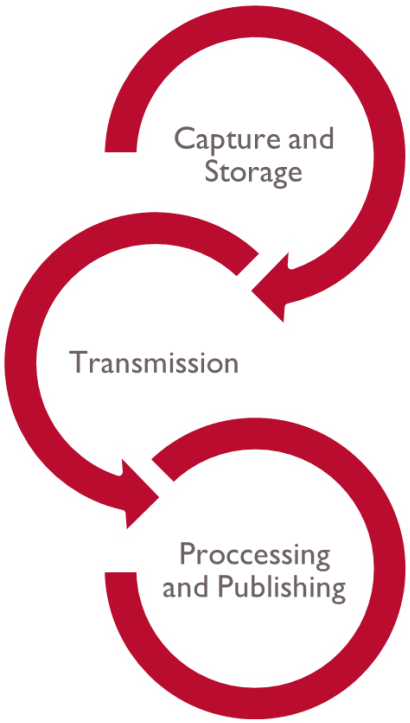
A fully automated RMS is characterized by minimal to zero human interaction, for example, when electronic voting machines (EVMs)[8] are deployed at polling stations. While there may be some paper

[7] Cobos-Flores, F. and McDermott, R. (2015). *Electoral Results Management Systems: Catalogue of Options.* United Nations Development Programme. https://www.ec-undp-electoralassistance.org/wp-content/uploads/2018/08/undp-contents-publications-electoral-results-management-systems-catalogue-of-options-English.pdf

[8] Electronic voting machines refer to systems that utilize electronic components for functions of ballot presentation, voter capture, vote recording, and in some cases, tabulation.

involved, such as with ballot marking systems[9], ballot scanning systems,[10] and EVMs with voter-verified paper audit trails,[11] EVMs are considered fully automated from a results management perspective, because the results are reflected in the digital domain without human interaction. Their storage, onward transmission, and processing are along similar, though not identical, lines to hybrid systems.

Results Management Process



A. Capture and Storage of Election Results

While results management processes vary across countries, regions, and systems, similar non-digital tools and digital technologies are used in every type of RMS. The first stage of the results management process is capturing and storing election results. This stage includes all activities related to preparing voting forms, compiling ballots cast (regardless of their format), and saving and storing them at the polling station- or precinct-level.

In the capture and storage stage of the election result process, several different tools can be used. Non-digital tools include pre-printed paper forms and no-carbon copy[12] paper forms. Most countries utilizing all-paper or hybrid RMS still use paper ballots. Most commonly, they are counted after the close of polls at the place of poll – i.e., the polling station or precinct. The information from the count is captured on one or more forms, known as results forms, tally sheets or protocols. The information on the results form will, at minimum, include the name and code of the polling station, the names of the candidates (or referendum choices), and the number of votes cast for each. The presiding officer's signature will typically be on the form. In all-paper or hybrid RMS, the signatures of the political party and candidate agents present will also be captured on the results forms to show their attestation of the accuracy of the form. It is very common to post one copy of the results form outside the polling station for public scrutiny. It is also common to share copies of the results forms

[9] A device that permits candidates to be reviewed on an electronic interface, produces a human-readable paper ballot, and does not make any other lasting record of the voter's sections.

[10] A device used to read the voter selection data from a paper ballot or ballot card.

[11] Voter Verified Paper Trails (VVPT) reference a mechanism that also provides physical paper records of voter ballots as voters have cast them on electronic voting systems. This paper trail allows voters to verify that their choice represented on the paper corresponds with the vote they cast on the machine. The paper trail allows for auditing of the voting record if necessary.

[12] No-carbon-copy (non-carbon copy or carbonless copy) paper allows the presiding officer to fill in just one form, then quickly provide identical copies as required. There is a practical limit on the number of copies per form – too many and the bottom copy may not be legible – local environmental conditions (temperature, humidity, availability of firm, flat surface) should dictate the choices.

with the political party agents and candidates present. Results forms may be printed in advance to fill out after ballot casting and may have security features integrated.[13]

Completed physical ballots also need to be secured for storage and/or transport. This often happens at the local tabulation center. The ballots must be stored in such a way that they can be used for post-election audits and court challenges. Physical chain-of-custody forms may be used for recording who has control of the ballots at any point in time and when transfers between parties occur.

In hybrid or fully automated RMS, digital technologies in the capturing sequence range from digital cameras, dedicated tables or mobile devices, bring-your-own-device (BYOD) smartphones, or "dumb" phones. BYOD is a catch-all term used to describe a policy where polling staff may use their own phones or smartphones to carry out one or more tasks associated with their work. An official (the presiding officer at the polling station level or an EMB official at higher levels) may use a computer (desktop/laptop) or a tablet-like device, or their smartphones[14] to capture the text and numerical data from results forms or to scan or photograph the forms.

The data and images captured this way may be stored locally or transmitted to central servers or a combination of both.[15] Cryptography can also be applied to data for protection and device storage, and removable storage can be used to store results ahead of transmission. Device storage includes traditional computer hard disks or newer solid-state drives (including handheld USB memory sticks), tablets, or mobile devices with storage directly integrated into them.

B. Transmission of Election Results

The second stage of the election management process is the transmission of election results. This stage refers to the steps and procedures related to transmitting the election results from the local level, that is, polling station, to the count center(s) for processing. Depending on the individual RMS, the election results may make multiple stops at the local, regional, or national levels for processing or verification. In cases where technology is used, cyber vulnerabilities emerge as results are transmitted over electronic infrastructure. Additionally, the physical security of results stored on electronic media can become important at this stage as well, as results are transported from one location to the next.

During the transmission stage of election results, the tools and processes used in election management, digital and non-digital, expand. Where no technology is deployed at a particular polling station, the Presiding Officer will seal the results forms and other sensitive materials in a tamper-evident bag (TEB) or

[13] The most common security features on printed election material include watermarking, Guilloche patterns, micro-text and anti-copying lines. Less common (and more expensive) are invisible features (ink, chemical watermarks) or highly visible features such as holograms.

[14] *See* the Pakistan case study in this paper for more details on this approach.

[15] Good practice is to adopt a "store and forward" approach. When connectivity is lacking or absent, the system may store data and form images locally. When connectivity is restored, data and images can be transmitted. Ultimately, removable media may be used to recover data when there is no connectivity. In Zambia, the system used whatever connection was available to send what that connection could support (for example, SMS for numbers only, mobile internet for numbers, 3G or 4G or Wi-Fi or Ethernet for numbers and images of forms).

tamper-evident envelope (TEE).[16] While they cannot prevent a bad actor from opening them, they will be visibly damaged or destroyed, bringing the tampering to the attention of the receiving electoral official. Once stored in a TEB or TEE, if no further counts are to be conducted for other elections held that day, the Presiding Officer will then proceed to the next level of the electoral administrative hierarchy, typically the location where the Returning Officer[17] for a constituency has an established count center. Depending on the size of the country, the count center might be a single national center or the first in one or more levels of aggregation. Other non-digital tools, such as ballot boxes with numbered seals, facsimiles (analog), or orally recorded through traditional public telephone networks or cellular devices, can be used to transmit results to the relevant central server or tallying station.

Fully automated and hybrid RMS use digital technologies such as cellular services (SMS/Unstructured Supplementary Service Data), mobile data networks, satellite communications, removable media, such as universal serial bus (USB), hard disk drive (HDD), solid-state drive (SSD) and secure digital (SD), Wi-Fi, ethernet, Bluetooth, cryptography, cloud services, and VPNs to transmit results to central servers or tallying stations. In hybrid RMS, a combination of non-digital and digital tools is typically used depending on the resources and locations of certain polling stations.

C. Processing and Publishing Election Results

The final stage of the election results management process is the processing and publishing stage. During this stage, the election management body processes election results for final verification before publishing them for public notice. Depending on the RMS and the election, this stage can be ongoing during the election management process, as election results are tallied, verified, and finalized at the local to national levels on and after election day.

The non-digital tools used in the processing and publishing stage of election results can include result forms, tally sheets, gazettes, and printed notices, which are usually publicly posted outside the polling station. Examples of digital tools used include:

- Electronic databases
- Electronic document management tools
- Generic statistical tools like Microsoft Excel
- Geographic Information Systems
- Election-specific software applications bought from vendors or custom developed by the EMB
- Servers
- Firewalls
- Routers

[16] TEB or TEE are, respectively, tamper-evident bags or tamper-evident envelopes. While they cannot prevent an attacker from opening them to access the contents inside, they are visibly damaged or destroyed by doing so, bringing the tampering to the attention of the receiving electoral official. The analogy with digital hashing (as a cryptographic "tamper evident" mechanism) might be useful for cybersecurity professionals.

[17] In multi-election scenarios, there may be multiple Returning Officers (one per race). This adds a level of complexity to the process. For example, in Kenya´s general elections, there is a Constituency Returning Officer for the National Assembly Constituencies. There is also a County Returning Officer for county assembly races.

Other hardware and software can be utilized depending on the particular RMS design in any given country. These tools are used to not only compile the data but protect it from manipulation and interference. For publishing election results, the RMS design of a particular election commission may utilize general internet infrastructure from commercial service providers or custom transmission systems that function via legacy telephone networks, or a hybrid system. Increasingly, social media is used to publicize results. There are also a variety of security tools utilized in the processing stages to prevent interference in the authentic distribution of accurate and final election results. What is published precisely will vary from country to country, and may range from a minimal notification of who won, through a more granular breakdown by region or district, all the way to detailed polling-station level results. Scans of original paper documents may or may not be published. Likewise, published results may be no more than scans of legal documents or may be in digital (data) formats allowing download and analysis. As the variety of approaches suggests, there are no internationally binding rules; nevertheless, the Open Election Data Principles are a useful framework in this respect.[18]

These three stages of the election results management process – capturing and storing; transmitting; and processing and publishing results – encompass a wide variety of RMS approaches. The next section provides a case study of a country that moved from an all-paper to a hybrid system and the complications that arose from implementing new technology and ensuring its proper usage. The mix and sophistication of the technology involved varies greatly depending on the technical maturity and sophistication of the RMS in any particular country and locality. This example highlights the complexity of the results management process and ways in which combining different digital and non-digital tools can lead to difficulties in tracking and managing the electoral process. Apart from ensuring proper usage of digital and non-digital tools in RMS, oversight of the requirements to help coordinate their usage through all three stages of the elections management process is also key.

LESSONS LEARNED FROM TRANSITIONING FROM AN ALL-PAPER TO HYBRID RMS – PAKISTAN

Pakistan's 2013 Elections: From an all-paper to hybrid RMS

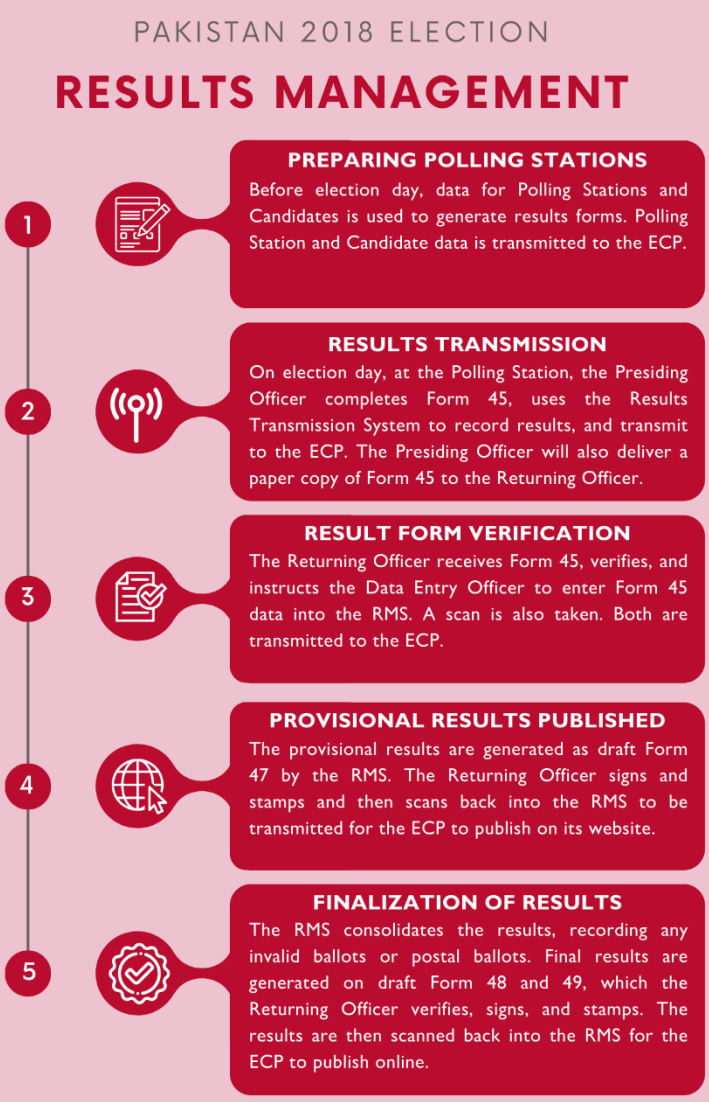
Prior to 2013, Pakistan's RMS was almost entirely a paper process. Ballots were counted at each polling station, copies of the results captured on paper forms[19] were posted outside the premises (making the information available in the public domain) and signed copies were shared with the party and candidate agents present. The Presiding Officers packed the paper forms, along with other sensitive materials, in tamper-evident envelopes, brought them to the constituency tally center, and submitted them to the Returning Officer for tallying.

Tallying was traditionally a largely manual and paper process, though some Returning Officers used tools such as Microsoft Excel to support their efforts. Once the constituency results were completed, signed paper copies were shared with party or candidate agents and posted outside the premises. Following the finalization of the results, the Election Commission of Pakistan (ECP) published them (as required by law) and posted some high-level results on its website.

[18] The Open Election Data Initiative (n.d.). *Section 2: Open Election Data Principles.* https://openelectiondata.net/en/guide/principles/

[19] Form 45 is the foundational form, completed at the polling station, of the results management process.

In the 2013 General Elections, the ECP, with the support of international partners,[20] deployed its sanctioned electronic RMS at the tallying center of each constituency Returning Officer. The new system allowed for data entry from polling station forms. All stored data and form images could be transmitted to central servers of the EMB. Despite the introduction of technology into the process, the 2013 RMS was merely a tool to aid the Returning Officer and facilitate oversight by the ECP; the legally and procedurally defined results process did not change. Without a clear legal mandate, and without the ECP mandating its usage (by instruction or regulation), not every Returning Officer used the system[21] and the ECP did not publish raw data or the scanned forms on its website. The lack of consistency across the process led to pressure from civil society and in response, the ECP called for all Returning Officers to make certified copies of all forms available. While this was not as transparent as the online publication of data and scanning of the forms would have been, it reflected an institutional desire for greater transparency.



2017 Elections Act: An introduction to legally mandated technology with RMS

The 2017 Elections Act explicitly addressed lessons learned by the ECP in its management of electoral results – making the use of technology legally mandated,[22] though the paper results remained the legal document. However, the 2017 Act also mandated the electronic capture and transmission of results from the polling station, which posed a significant timing challenge given the law was passed in 2017 and the elections were scheduled for mid-2018. For the field-deployed solution, the ECP reached out to NADRA (Pakistan's civil registry), resulting in essentially two separate results management systems on election day – one (known as the Results Transmission System, RTS) used by the Presiding Officer at each of the over 130,000 polling stations and the second (known as the Results Management System, or RMS) used by the

[20] The mechanism for international technical assistance to the ECP in this instance was a UNDP project, resourced using a basket fund with multiple donors, including USAID, UK, Australia, Japan, the European Union, Norway and Switzerland.

[21] It is estimated that 70 to 80 percent of ROs used the system to send some or all data to ECP HQ. (Sources include internal UNDP reporting and EU EOM observer reports.)

[22] The law also required RO to meet an 0200hrs deadline for electronic submission of their results.

Returning Officer at each of 269 National Assembly constituency tally centers and a further 571 Provincial Assembly tallying centers.

The short turnaround for implementing the Elections Act ahead of the 2018 elections made it impossible to procure and deploy dedicated devices for RTS. Therefore, the ECP's solution allowed the Presiding Officers to use their own (or a borrowed) smartphone, with a bespoke RTS application installed, to capture and transmit results data accompanied by a photographed image of the results form. There was also inadequate time to conduct training, pilot tests, large-scale simulations, or mock elections to test the RTS. On election night, many problems surfaced, with delays in RTS used by the Presiding Officers affecting the work of Returning Officers, none of whom met their legal deadline for the electronic transmission of provisional National Assembly results. The ECP abandoned the RTS at midnight on election day and focused on the movement of paper results to the constituency-level, and subsequent tallying, verification, and transmission of results via RMS. Despite missing their transmission deadline, over 95% of Returning Officers transmitted provisional results using RMS within 36 hours of the close of polls.[23]

Key Takeaways

Despite a number of allegations[24] of attempts to manipulate the electoral process, no evidence has emerged of any type of cyber attack on RTS or RMS, leading most knowledgeable commentators to conclude that unrealistic timelines, poor planning, testing, and training, coupled with inadequate provisioning of telecommunications links and server capacities combined to make RTS less than successful that night. As happens in many countries where the General Elections are the first - problematic - use of a new information system, subsequent by-elections see the system perform as designed. This is true for Pakistan, where RTS was used without problems in many by-elections that followed the 2018 General Elections.[25]

Section III: Threat Actors and Their Motivations

After discussing the main stages of results management systems and the complex coordination required across the different stages regardless of the level of technology involved, it is important to discuss the various threat actors and their motivations for targeting these systems. Two motives lead a variety of actors to attack (or attack the credibility of) election results management systems. The first is to change the result of the election so that a preferred candidate or party (or referendum option) prevails, despite the will of the electorate. The second is to undermine the credibility of the results management process and, therefore, the entire electoral process by eroding public and political confidence to the point where the election results are rejected. Since results management comes at the very peak of an electoral cycle, protecting results forms, data, tools, and systems are critical priorities around which EMBs build cyber capacities and safeguards. As outlined above, the RMS often has components that are accessible to the

[23] Author was in Islamabad throughout the election period.

[24] Wasim, A. (2018, August 2). *RTS controversy likely to haunt ECP, Nadra for a long time.* Dawn. https://www.dawn.com/news/1424394/rts-controversy-likely-to-haunt-ecp-nadra-for-a-long-time

[25] ECP has developed a new RMS since 2018 and, while there are significant similarities with the systems discussed in this case study, there are also differences. ECP's website still contains the 2018 outreach materials (at the time of writing). https://www.ecp.gov.pk/frmGenericPage.aspx?PageID=3157

public online. Combined with other factors, this accessibility makes RMS and the results data contained therein an attractive target.

A. Foreign State Actors and Advanced Persistent Threats

There are multiple reasons why malicious actors working from or affiliated with foreign states target results management systems. These range from a desire to alter or influence the outcome of an election to, more commonly,[26] undermining public and political party confidence in the election itself. There are no known attacks that have been directed solely at results management systems, but there have been many on (or probes into) elections management information systems and infrastructure. Many of these systems are used to store, process, and publish results, in addition to voter registration, elections logistics, candidate nominations, and other electoral applications.

In many countries (Kenya 2011, Ukraine 2014), despite the lack of evidence of actual damage to electoral information systems and data, the erosion of trust arising from real (Ukraine) or alleged (Kenya) cyber attacks has genuinely harmed the elections and democracy there.

While few attacks on RMS are directly attributed to foreign Advanced Persistent Threats (APT), it is entirely reasonable to regard RMS as attractive targets for this category of malicious actor.

ADVANCED PERSISTENT THREAT, OR APT

As defined by National Institute of Standards and Technology (NIST):

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."[27]

APTs have scanned and targeted other election infrastructure such as voter registration systems. Before the 2018 parliamentary elections, Colombia's national voter registration web platform, which contained 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.[28] In 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) 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.[29]

---

[26] The latter reason may be more common because, in the case of the former, it is not enough to merely change the results; one must do so ***without detection*** – a greater challenge. A clue to the magnitude of changing results without detection lies in the prizes offered in Switzerland's 2019 Public Intrusion Test of its internet voting platform. The prize for changing a vote was almost half a million Swiss francs, while the prize for doing so without the possibility of being detected was over one million Swiss francs. *See* IFES. (2019). *Feasibility Study on the Introduction of New Electoral Technologies for Ukraine.* https://ifesukraine.org/wp-content/uploads/2019/04/IFES-Ukraine-Feasibility-Study-on-the-Introduction-of-New-Elections-Technology-for-Ukraine-v1-2020-02-13-Ukr.pdf

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

[28] 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

[29] 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

Attributing 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 U.S. voters during the 2020 elections. Moscow similarly denied that it had been attacking American electoral processes.[30] 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.[31] While these instances provide examples of an APT on other elements of the election process, the accessibility of an RMS makes it a vulnerable target. Unfortunately, foreign state actors and APTs may be particularly well-resourced and motivated to conduct attacks on RMS to exert (or threaten to exert) influence on public trust or the election process itself.

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. Michael Amoah's detailed examination of four recent African elections[32] explores the theory that "high-staked presidential elections in winner-take-all political systems tend to generate enormous potential or propensity for incumbent interference in EMB operations." As such, domestic threats emanating from or within the government need to be taken seriously. The manipulation of results is easier to undertake, and harder to detect, in situations where election administration is directly controlled by incumbents or the RMS lacks transparency and accountability.[33]

Where the RMS is sufficiently tamper-evident and enough government control of the underlying systems exists, the first motive (manipulation of results to achieve the desired result) may not be deliverable, so the fallback position of undermining the process remains an option. One way a malevolent government actor could undermine the system would be to undertake false flag cyberattacks to shift the blame to external actors to erode public trust in the process. In places where there are fewer overlapping checks and/or weak civil society, government actors may try to exert undue influence on elections and choose cyber means to do so.[34]

---

[30] Collier, K. (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

[31] 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

[32] Amoah, M. (2020, January). *Sleight is right: Cyber control as a new battleground for African elections*. African Affairs, *119*(474). (p. 68–89). https://doi.org/10.1093/afraf/adz023

[33] OAS Final Report: Honduras General Elections 2017. https://www.oas.org/eomdatabase/moereport.aspx?lang=en&id=396&missionid=473

[34] Fisher, M. (2013, October 9). *Oops: Azerbaijan released election results before voting had even started.* The Washington Post. https://www.washingtonpost.com/news/worldviews/wp/2013/10/09/oops-azerbaijan-released-election-results-before-voting-had-even-started/

C. Criminal Groups

Unlike voter registration databases, whose contents may have commercial value for criminal groups, there is no market for election results data – because these are, for the most part, in the public domain. When expensive equipment such as laptops, scanners, tablets are distributed to the field as part of an RMS, these items may be attractive targets for burglary, particularly if facilities where they are stored are not well protected, or they are vulnerable during transfer. Equipment can be resold on the local black market. The theft of a significant number of RMS devices could constitute a sort of "denial of service" by preventing the RMS from being used in polling stations or at count or tallying centers. Nigeria's Independent National Electoral Commission (INEC) experienced such a theft leading up to the 2010 voter registration exercise.[35] Criminals can also be hired by foreign entities to direct attacks against important infrastructure, such as election systems. Russia has used both criminals and politically motivated groups to carry out proxy attacks against various target countries.[36]

Various reliable media have detailed alleged election interference utilizing paid criminals to hack campaigns, manipulate social media, and perform other criminal acts to advance one candidate over another.[37] While the detailed acts focused on gathering information from target individuals and organizations, it is likely that a market for skills to attack election results management systems could also develop if threat actors decide to focus further on this element of elections. Recent findings from Google's Threat Analysis Group and IBM's Security X-Force suggest "blurring lines between financially motivated and government-backed groups in Eastern Europe, illustrating a trend of threat actors changing their targeting to align with regional geopolitical interests."[38] This amounts to a sort of malevolent pro bono approach by certain criminal groups, perhaps seeking to curry favor with state actors. Election results management, with the vulnerabilities inherent to its multi-stage process, thus, could find itself as the target for such criminal activity as geopolitical and financial interests coalesce around disrupting elections and their proper execution, even if the intent is to simply mobilize public discontent and disillusionment with democratic government.

D. Non-State Political Groups and Hacktivists

Hacktivists (defined as hackers with explicit social or political motivations) and non-state political groups may target RMS for various reasons, for example, to damage the credibility of an EMB, or to attempt to

---

[35] 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 of machines containing 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/.

[36] Russia has reportedly diverted technically proficient criminals to work in cyber operations instead of prosecuting them. That strategy and other recruitment strategies are reported in: Kramer, A. 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

[37] Robertson, J., Riley, M., and Willis, A. (2016, March 31). *How to Hack and Election: Andrés Sepúlveda rigged elections throughout Latin America for almost a decade. He tells his story for the first time.* Bloomberg https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[38] Bureau, P.M. (2022, September 7). *Initial access broker repurposing techniques in targeted attacks against Ukraine.* Google Threat Analysis Group. https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

undermine stakeholder trust and confidence in an election. By targeting the election, specifically the results management process, hacktivists, like the other threat actors, can influence the election result, whether it be the actual voting result or general sentiment surrounding the election which, then, can feed into a larger cause or issue the hacktivist is trying to promote. Whether ideological, social, or political, hacktivists' motivation to attack RMS lies in the accessibility and public nature of the actual election process itself. In the Philippines, for example, two hacktivist groups targeted the EMB to signal discontent with the overall electoral process and concerns about the security of the precinct count optical scanners in 2016.[39] Given a social or political cause is usually associated with the actions of hacktivists, the motivations, grievances, or goals are usually well-signaled or communicated, even if hacktivists hide their identities.

However, an important caveat regarding hacktivists' and non-state actors' motivations for targeting election processes 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 foreign actors. For example, in 2019, Indonesia's voter registry database 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 among local groups that were using foreign IP addresses to falsify their location.

Attribution of cyberattacks is notoriously difficult and time-consuming. In the critical hours after polls close, it is almost impossible to attribute any cyberattack to a specific group or actor. By the time any attribution can be made, the damage may be done – RMS operate in highly time-bound circumstances with as little as seven days in some jurisdictions to certify final, complete, official results. Furthermore, in some countries, preliminary results can be released as early as election night or the day after, and the public, media, and candidates pay the most attention to those results, regardless of verification and finalization, only exacerbating the real-time significance of the results management process.

E. Insiders

There is no "one profile fits all" when it comes to insider threats, and the usual motivations (sabotage, theft, fraud) are not always a natural fit when it comes to election management processes. However, insiders can be described as people who "bypass physical and electronic security measures through legitimate means every day."[40]

Discussion of insider threat motives is largely speculative, given that undermining EMB systems and safeguards is covert and opaque, and few instances have been documented. However, individual or collective threat actors could operate from within EMBs – as staff, consultants, contractors, volunteers, or trusted partners – to target results management systems for any number of reasons, including political leanings, personal grudges, or financial gain. This sort of abuse of access by employees and former employees can be hard to prevent and detect. While insiders are often defined as individuals that have access and harbor ill intent, it is important to understand the risk of insiders that have been coerced into cooperating with threat actors. Election officials can be threatened or coerced to provide access or

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

[40] Capelli, D., Moore, A., and Trzeciak, R. (2012), "The CERT® Guide to Insider Threats." Addison Wesley, ISBN 978-0-321-81257-5. (p. 1).

leveraged to breach confidentiality, integrity, or availability of systems. Shortly before Election Day in Kenya in 2017, for example, the EMB's IT manager was tortured and murdered, allegedly in order to obtain passwords to the Independent Electoral and Boundaries Commission's (IEBC) sensitive databases.[41] Seemingly, the IT manager's statements that he would safeguard election systems from interference made him a target.[42] This event left insiders at elections management bodies around the world fearing for their lives. It is, therefore, incumbent on EMBs not only to protect their RMS from insider threats but also their staff from becoming victims of intimidation and coercion.

The growing vulnerability of electoral information systems to insider attacks was acknowledged by former U.S. Election Admission Commission (EAC) official Ryan Macias when he said "…. since 2020, the coordinated efforts to have threat actors run for office, apply to be election officials and volunteer as a poll worker or observer should be treated as national security concerns."[43]

There is at least one well-known – but little publicized – case of a privileged insider, that, for the purposes of this briefing, will remain unnamed, who attempted to manipulate election results data at the database table level. In anticipation of such insider attacks, the designers of the results management system included triggers that silently alerted senior managers when data was altered in an unusual manner. The offender was confronted, and quietly resigned. No election results were changed.[44]

Many countries allow political parties and candidates to nominate poll workers, and the composition of EMBs is often a mix of members from government, opposition, civil society, and judicial sources. Less frequently, some EMBs are required to have a mix of political party-appointed technical staff in their secretariats (Puerto Rico, Georgia, El Salvador). In other cases, staff are partisan, despite being hired off the street. While there is no reason to assume that a professional appointed by a political party will be a greater threat than someone recruited off the street, the optics of partisan EMB staff make it that much more important that the design and operation of the results management systems be secure, transparent and accountable.

Section IV: Cybersecurity Risks Across the Results Management Process

This section will focus on cybersecurity risks to RMS that are under the purview of the EMB. The following is not a comprehensive list of risks, but rather a discussion of RMS-specific attacks. It is important to note that the timely and accurate management of election results encompasses only one of an EMB's main priorities during the election process. Issues, such as misinformation and disinformation, are not covered despite constituting other important elements to consider during this process.

---

[41] Omolo, K. and 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

[42] Ibid.

[43] Cassidy, C. (2022, February 25). *Attacks from within seen as a growing threat to elections across the U.S.* Los Angeles Times. https://www.latimes.com/world-nation/story/2022-02-25/attacks-from-within-seen-as-a-growing-threat-to-elections-across-the-u-s

[44] Sources were international technical assistance providers directly involved with this case.

A. Capture and Storage of Election Results

KEY RISKS:

- Deliberate or coerced manipulation of results by poll workers
- Denial of service attacks that prevent information technology infrastructure from being utilized
- Manipulation of results at the point of capture (compromised devices)

As previously discussed, the "insider threat" posed by members of EMB staff or one of the many thousands of ad-hoc poll workers hired for each election event remains a key risk. The counting and completion of results forms (including the capture of those forms and data-entry of results) should be observed by everyone present, and the completion of forms witnessed by political party and candidate agents and corroborated by their signature. Nevertheless, problems can arise with the paper and digital processes due to deliberate or coerced behavior by Presiding Officers.

Where dedicated devices are provided by the EMB to poll workers for the capture of data and images from results forms, the EMB can have significant control over the configuration and protection of those devices. When the bring-your-own-device approach is adopted, the burden of securing the environment increases and can also increase the risk of cybersecurity attacks. Without the same level of uniformity and consolidation among the technology used in the RMS process across the various polling stations, the risks of cyberattacks, manipulation, and human error increase significantly.

Solutions implemented in the field, such as laptops, tablets, or even the poll workers' own devices, at the local polling station or district level during the intermediate results tabulation and consolidation part of the capture and storage phase open the RMS processes up to supply chain attacks. Such attacks seek to insert, alter, or compromise devices and software not at the point of use but during their manufacturing or delivery, or through third-party connections or supplier-based means. The attacks may include altering the software or firmware of equipment to change data during or after capture. In addition, any contracted services that are used for data storage or, as discussed below, for transmission are potential vectors for cybersecurity vulnerability. Vetting, monitoring, and managing vendor-introduced risk is something EMBs will need to increasingly deal with if movement to cloud-based solutions gains further momentum in the election technology space.

B. Transmission of Election Results

KEY RISKS:

- Denial of service
- Manipulation of results in transmission
- Deliberate or coerced false attribution

The vulnerability of paper results to being intercepted and manipulated, as discussed in the introduction, has given rise to integrity mechanisms such as tamper-evident envelopes and, more recently, the use of digital technologies to capture, store and transmit results from polling stations and tally centers. All technologies used for transmission, including digital infrastructure, are subject to potential attacks, most simply by preventing transmission. It is harder to manipulate results data while it is being transmitted if adequate cyber protections, such as encryption, are in place. The most immediate risks are related to preventing transmission or manipulating the data before and after transmission has occurred. In the past, paper results forms were intercepted, adjustments made, and the forms would be submitted at the next stage in the processing as legitimate results. This

sort of risk still exists, but threat actors are now more likely to focus on the prevention of transmission.[45] Guarding against risks during the transmission phase requires mitigating attacks against data availability while also verifying data integrity. It is also necessary to implement strong protections to ensure confidentiality during transmission and storage (like encryption, as mentioned earlier).

In countries where governments are prone to blocking the internet in response to real or perceived seditious online activity, legitimate traffic (such as election results) is also often blocked as well. Such unintended consequences can slow down results management systems as paper and data must move at the same, slower speed.

Less dramatic, but equally problematic, is the increased traffic on cellular networks around polling stations, intermediate tally centers, and national results centers. Presiding Officers in busy urban polling stations may struggle to get a reliable signal when the time to transmit results data and form images comes.

RMS SHORTCOMINGS FROM THE 2017 KENYAN PRESIDENTIAL ELECTIONS

The Shifting Burden of Proof

The choice of Kenya as a case study is driven by the evolution – visible from 2017 to 2022 – of the institutional responses to the specific allegations of compromised RMS used during the Presidential Elections in both years. As advocated in the Kriegler Commission Report[46] which followed the significant post-electoral violence in 2007, Kenya began to introduce technology into its electoral processes. In 2010, the EMB in Kenya piloted biometric voter registration (BVR) and introduced further use of election technology for the General Elections in 2013 when the IEBC introduced a paper/electronic hybrid model of RMS. Paper results forms were completed at the polling station following the count and copies of these forms were shared with political party and candidate agents. A multi-election application run on simple cellular headsets logged the results from these forms and transmitted them to central servers and servers at the county level. After issues with delayed transmission and election results processing in the 2013 elections, Kenya's IEBC invested heavily in a new, highly integrated solution – the platform, called KIEMS (Kenya Integrated Elections Management System) was envisaged for all three key electoral processes – biometric voter registration, biometric voter verification, and electronic results management.

However, in the 2017 Presidential Election, the shortcomings in the transmission stage of the election results process led to a loss of faith in the integrity of the entire election. Allegations of manipulation of election results during transmission and processing led to a Supreme Court of Kenya (SCoK) case that ultimately overturned the results of the election. During the proceedings, the petitioner established that some illegalities and irregularities had occurred. These were not so great (in terms of number of votes) to overturn the result of the election. However, the SCoK ruled that the burden of proof had shifted to the defendants. This meant that the EMB had to prove that its systems were ***not*** compromised. Through the proceedings, it was clear the EMB,

[45] Regarding interception of communications, *see* "Man-in-the-Middle Attacks" (MITM) in the table presented below for tactics, techniques, and procedures noted within this briefing paper.

[46] Independent Review Commission on the General Elections held on 27 December 2007 (Kriegler Commission Report). The Report recommends integration of technology into Kenya's electoral processes for registration, identification of voters and transmission of results." 2022 Supreme Court of Kenya. (2022). *Judgment* (p. 7).

with its ill-defined protocols and documentation of the process, could not provide definitive evidence of the security of its electronic transmission of results from constituencies. Thus, the elections were overturned based on the IEBC's inability to prove the security and integrity of its results management process to the Court's satisfaction.[47]

C. Processing and Publishing of Election Results

KEY RISKS:

- Manipulation of results on servers and websites
- Cyber vulnerabilities in internal EMB results management and processing systems
- Denial of service
- Social engineering
- Phishing
- Coercion

Attacks on EMB servers and websites are well documented by journalists and academics and cited throughout this briefing paper. The more public-facing an asset, the more attractive it is, not only because it is likely more easily accessed for reconnaissance and exploitation, but also for the visibility an attack may garner, undermining the electoral system, should that be a goal of the attacker. Nevertheless, a RMS operation's internal server or network is equally vulnerable to attack. If the EMB has limited knowledge or resources, it may, understandably, focus on protecting public-facing servers. Furthermore, when an EMB has regional or other sub-national servers, they may not enjoy the same level of physical or administrative protections, adding to the risk. So-called "stand-alone" hardware and networks that are not connected to the internet are not inherently secure and can be targeted using tactics and techniques such as via insiders, or "back-doors," before the hardware or software is delivered.[48]

Risk to information assets that are used to process and manage results (such as those used to aggregate results at intermediate steps) can be vulnerable to exploits tailored to the specific customized or niche software and hardware used within the relatively boutique election software and hardware market (or, in the case of systems, developed by an EMB "in-house"). In some ways, this is analogous to the types of risks considered within the "operational technologies"[49] segment of cybersecurity in industries such as manufacturing or the energy sector. A lot has been written on the vulnerability of Supervisory Control and Data Acquisition (SCADA), for example, and there are lessons to be drawn from this category of vulnerability and risk management techniques.[50]

DDoS attacks can also threaten the processing and publishing of election results. Larger countries whose election results websites show demand in the millions of hits per hour on election night and in the

[47] Four of the six Justices on the Supreme Court bench hearing the electoral petition ruled against the IEBC. The remaining two issued lengthy dissenting opinions.

[48] *See* "Supply chain attacks" in the table of tactics, techniques, and procedures later in this briefing paper for further information.

[49] Operational technologies (OT) are systems or devices that interact with the physical environment. This can include systems and devices used in industrial control, building management, fire control, and physical access systems. Traditionally, these sorts of technologies have not received the same level of security focus and protection as more traditional computer hardware and software, leading to vulnerabilities that can have spill-over effects, especially in the case where the systems in question perform essential functions. The comparison to election systems rests on the fact that both election technologies and OT may not have been designed with security as a major focus, which may lead to vulnerability and risk.

[50] United States Cybersecurity & Infrastructure Security Agency. (n.d.). *Alert (AA20-205A) NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems*. https://www.cisa.gov/uscert/ncas/alerts/aa20-205a

following days may use Content Distribution Networks (CDN)[51] to mitigate DDoS. However, even these solutions are not invulnerable.[52] Simply slowing down the availability or limiting widespread knowledge of election results may cause issues, making such tactics attractive to malicious actors.

Social engineering[53] or phishing attacks to steal the credentials of all EMB assets, including social media accounts, are aimed at gaining access to impersonate official sources. While many social media platforms lock an account after too many unsuccessful login attempts, the fact that there is no serious consequence for attempting to log in makes them tempting mechanisms for disrupting EMB communications.

Section V: Potential Types of Attacks and Risks

Cyberattacks 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.[54] TTPs are important to consider since certain ones can help distinguish one threat actor from another. Discussion of cybersecurity TTPs could easily focus on their technical dimensions, but this paper provides an introduction to how various threat actors employ specific methods, tools, and actions that they tend to favor.[55]

Information technology infrastructure can be exploited through a variety of techniques and tactics at every stage of the results management process. When RMS incorporate field-deployed technologies (into the polling station or center), the attack surface, that is the multitude of places an attacker can potentially enter your systems and networks, grows substantially, and the number of personnel requiring access grows as well, even as the level of computer (and cyber-hygiene) literacy diminishes due to the increase in technically unsophisticated users. With more EMBs turning to third-party solutions staffed by oftentimes inexperienced and underqualified professionals, unprotected or poorly protected databases are a high risk. Additionally, insiders can facilitate data access to criminal groups.[56] The following table highlights some of the most common tactics and techniques that can lead to compromised electoral technology infrastructures.

---

[51] Content Distribution Networks consist of commercial internet infrastructure providers that enable wide accessibility of customer content/data by distributing copies across different geographic data centers to help speed up delivery and ensure redundant access.

[52] Culnane, C., Eldridge, B., Essex, A, and Teague, V (2017). "Trust Implications of DDoS Protection in Online Elections," proceedings of Second International Joint Conference, E-Vote-ID, Bregenz, Austria.

[53] Social engineering refers to the exploitation of human nature to gain access to personal information. This approach can utilize different tactics that are touched on in the table below.

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

[55] 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, MITRE. (n.d.). Att&ck. https://attack.mitre.org

[56] In 2020, a criminal group distributed an official PDF from the Indonesian election commission, the KPU, online. The full investigation was not published, but it was alleged that the criminals were the recipients of an internal leak. *See,* Nugraha, R. M. (2020, May 22). *KPU Alleged Hacking Leaves 2.3 Million Personal Data Compromised*. https://en.tempo.co/read/1345108/kpu-alleged-hacking-leaves-2-3-million-personal-data-compromised

COMMON TACTICS, TECHNIQUES, AND PROCEDURES	
PHISHING	This type of attack tricks users to disclose sensitive information, such as usernames and passwords, or allowing 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.[57]
SPEAR-PHISHING	This tactic is a far more targeted variant of the phishing technique. Often states and sophisticated actors will tailor content or messaging based on intelligence and specific information about the target to make it more likely they will be tricked. An insider with elevated privileges on RMS becomes a high-value target to threat actors. They may also target vendors with privileged account access for performing essential business functions and use that access to target the main entity's systems. An EMB's technology vendors, logistics providers, and third-party service providers must have robust cybersecurity.
INTERCEPTION AND COMPROMISE OF PHYSICAL DEVICES	This tactic may occur in RMS 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 can be easily resold on the black market or dark web. Relevant examples of theft have been reported in Hong Kong,[58] the Philippines,[59] Malawi,[60] Canada,[61] and the U.S. (Atlanta).[62] Access to the physical devices where the data is stored may allow malicious actors to manipulate results data that is not adequately encrypted. Specially crafted malware can be developed and injected via USB, allowing for further manipulation. Access to the RMS devices, even for a few seconds, can compromise the integrity of the results data. In 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.
TARGETED BOTNET OPERATIONS	Botnets are collections of compromised internet-connected computers 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. These DDoS attacks result in the targeted sites going down and becoming inoperable from a combination of already peak loads of visitors due to the level of public and stakeholder interest in election results.[63]
WATER HOLING	This type of attack uses fake websites that look legitimate or seem to serve a legitimate purpose but in fact, allow malicious actors to exploit users. Sometimes attackers set up websites that look similar or identical to legitimate companies' or governments' websites. Fake results websites can fuel rumors and undermine confidence in the election process.

Table Continued on Next Page

[57] Robles (2019)

[58] Ng, Y. S. (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

[59] Bueza, M. (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

[60] Sangala, T. (2018, October 20). *Voter registration 'kit' stolen.* The Times Group. https://times.mw/voter-registration-kit-stolen/

[61] 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

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

[63] 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., and 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

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 the password on professional accounts associated with that individual. This is of particular concern when an EMB adopts a bring-your-own-device (BYOD) model in an RMS.[64]
SUPPLY CHAIN ATTACKS	Supply chain attacks compromise hardware and software components before they are used (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.[65] 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. An example would be checking the SIM cards often provided to EMBs as part of a field-deployed RMS.
SOCIAL ENGINEERING	Social engineering often relies on non-technological means and exploits 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 personal identification numbers, or PINs. Physical threats and intimidation are frequently directed at elections management body staff and ad-hoc workers. The more field-deployed technology is used (for example, at the polling-station level) in RMS, the more personnel can be targeted for potential social engineering attacks.
MAN-IN-THE-MIDDLE	A MITM attack consists of intercepting communications between users and a legitimate destination to read or change the communication before relaying it, without compromising the destination website or system. RMS and other network-connected devices can have their communication intercepted by devices used near or at the polling station. Devices that use wireless connections that are not well encrypted are particularly at risk.
RANSOMWARE	The techniques discussed above are oftentimes leveraged to compromise networks to deploy software that encrypts the data on target systems. This is known as a "ransomware" attack. Threat actors may then contact the victim and offer to decrypt their data for a fee. The tactic can also be used for destructive attacks that delete information or cause other negative effects.

Section VI: EMB Approaches to Secure Results Management Processes

Effective cybersecurity responses are not spontaneous. EMBs must take ownership of their cybersecurity to secure their results management process, drawing on the resources and skills of other agencies in an emergency. Good practice and mitigation strategies are critical to RMS cybersecurity. This is particularly true when there are issues concerning an EMB's independence in a computer incident response scenario and when elections infrastructure is declared to be critical national infrastructure, as certain critical national infrastructure can be used in the RMS process. For this reason, and for security and objectivity, any use of commercial or third-party providers, that is, other involved entities both public and private, must be identified in advance and the appropriate measures built into the EMB's RMS strategy to avoid adverse political ramifications. For example, in countries where a National CERT (Computer Emergency Response Team) is relied on by an EMB to respond to a cybersecurity incident, there is a possibility this

[64] For example, Pakistan's RTS. *See* the case study in Section II of this paper.

[65] 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

could lead to a real or perceived compromise of independence. Especially if the National CERT is associated with the military, national police, or other parts of the state apparatus.

To ensure security and political neutrality, the EMB must ensure that it has its own technically skilled and trained personnel who can lead in an incident response scenario and who can communicate effectively with EMB senior managers and commissioners. As IFES has found, it is "imperative in the modern era of democratic elections that an electoral leader proactively consider the potential range of exposure to crises and prepare the institution to mitigate and manage them."[66] An EMB should utilize a "crisis management cycle approach" to enable it "to move away from being reactive and tactical toward a more strategic state of readiness that anticipates, plans for, mitigates and manages risk in ways that allow the organization to resolve and successfully emerge from crisis."[67]

There are two challenges oftentimes faced by EMBs in times of crisis, whether directly related to results management or other stages of the election cycle. First, non-specialist EMB staff members and their volunteers tend to lack a general understanding of utilized technology and associated jargon as discussed by senior EMB officials and their spokespersons. As is common, poll workers and EMB staff on the front lines are not necessarily familiar with all aspects of the RMS process and the technology associated with it. Second, the often-confusing nomenclature surrounding election results – "official," "provisional," "preliminary," "partial," "complete," "final," "verification," "certification" – requires careful navigation, through which EMBs must pay proper attention when faced with an issue or active threat during the results management process. Improper usage can lead to avenues for disinformation, revisions, or other issues related to public perception and accuracy.

In a crisis, an EMB cannot simply hand over responsibility for its infrastructure, data, processes, and communications (meaning media, public, and stakeholder communications) to a third-party agency. This is true even if that agency is the designated government or public agency with overarching responsibility for cyber defense and responses to attacks on critical national infrastructure. The International Institute for Democracy and Electoral Assistance (IDEA) has also found that elections and interagency collaborations pose a risk of controversy, citing an example from Romania where the EMB collaborated with an intelligence agency with legacy trust issues.[68] Collaboration with institutions with historically weak public trust is a major concern for EMBs in countries without a consolidated democracy that has a strong rule of law, privacy protections, and institutional transparency.

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 take inventory of electronic information devices and the sensitive data they hold; assess the risks of these assets, along with strengths and weaknesses of their current cyber defenses and

---

[66] Shein, E., Ellena K., Barnes, C., and Szilagyi, H. (2020 February). *Leadership in Crisis: Ensuring Independence, Ethics and Resilience in the Electoral Prrocess.* IFES and USAID publication. https://www.ifes.org/publications/leadership-crisis-ensuring-independence-ethics-and-resilience-electoral-process-0

[67] Ibid.

[68] "Romania: well-established close cooperation on auditing, but debate about cooperation with intelligence services." *See* van der Staak, S. and Wolf, P. (2019). *Cybersecurity in Elections: Models of Interagency Collaboration.* International Institute for Democracy and Electoral Assistance (IDEA). https://www.idea.int/publications/catalogue/cybersecurity-in-elections?lang=en

capacities; and then prioritize mitigation efforts.[69] Some overarching security considerations include ensuring that EMB staff and others – including political party and candidate agents, citizens and international observers (who may conduct parallel vote tabulations), and the voting public – play their role in protecting the integrity of the results management processes. This includes third-party vendors, who need clear guidance and the skills to prevent and respond to cyberattacks. Specific action items may include:

- Carefully vetting potential bidders during tender processes to identify security risks.
- Defining the role(s) of the vendor so the EMB remains in control of the process at all times and remains accountable should a problem arise.[70]
- Providing clear, formalized security requirements to third-party vendors providing devices used for the capture, storage, transmission, processing and presentation of results, and ancillary services. This includes ensuring systems are designed with the security features necessary to include robust access control, identity management, logging, and alerting capabilities for prevention, response, and an audit of election results.

Introducing controls against common attacks such as phishing and spear-phishing (e.g., providing EMB staff and data clerks responsible for RMS with training and resources on these types of attacks, and how to identify them and report them) is critical. For DDoS attacks, controls include incorporating services that help recognize and filter legitimate traffic and requests from illegitimate ones meant to overwhelm, slow, or interrupt services. In addition, in the face of public or legal scrutiny, EMBs should be prepared to:

- Procure or develop RMS that are maximally transparent to facilitate easy, independent, third-party validation of results, thereby staving off potential electoral petitions or disputes.
- Procure or develop RMS that are comprehensively disclosure-ready[71] in anticipation of court orders to that effect.
- Conduct and rigorously document appropriate cybersecurity testing well in advance of election day.
- Have staff and systems ready for rapid response to court-ordered disclosure.
- Plan and rehearse redundant operations, possibly with backup paper procedures prepared.

These measures require considerable knowledge of legal proceedings, rules of evidence/disclosure, and related matters. That is why EMB should ensure that the procurement, deployment, and operation of RMS are undertaken by multi-disciplinary teams including legal offices, not just staff from IT and Electoral

[69] For further information regarding security controls and risk management frameworks, *see* Chaudhary, T., Chanussot, T., and Wally, M. (n.d.). *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document.* https://pdf.usaid.gov/pdf_docs/PA00ZK5H.pdf. 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; and European Union Agency for Cybersecurity, *ENISA Risk Management/Risk Assessment Framework*. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework

[70] Goldsmith, B. and Ruthrauff, H. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. IFES, National Democratic Institute (NDI), and USAID publication. (p. 62). https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf

[71] Electoral Dispute Resolution is typically highly time bound. Rather than wait until a court orders disclosure during an electoral dispute litigation, EMBs should anticipate all possible disclosure orders and ensure well in advance of election day that all possible system documentation, test or audit reporting, logs, data, key management, chain-of-custody and related information are readily available.

Operations departments. Additionally, to further capacity and institutional knowledge, EMBs should ensure adequate training is built into election preparations to prepare poll workers, Presiding Officers, and Returning Officers for their core responsibilities in the results management process ahead of election day.

LESSONS LEARNED – THE KENYAN 2022 PRESIDENTIAL ELECTIONS

A Clearly Defined RMS

Following the overturn of the 2017 presidential elections in Kenya, the IEBC faced a similar challenge to its RMS in the 2022 presidential elections five years later. However, IBEC was prepared this time. After another wafer-thin margin in the Kenya Presidential Election, the losing candidate once again petitioned the ScoK, submitting large quantities of evidence of irregularities. One of the more sensational allegations was that of a MITM attack – a so-called "staging" server where results from polling station KIEMS devices were intercepted, altered, and then sent on to the back-end servers.

The SCoK made a comprehensive order for scrutiny[72] of the process, the paperwork, IEBC's RMS, and other aspects of the election. The IEBC was able to provide the plaintiff with much of what was requested. Notably, the IEBC did not give administrator credentials (from RMS servers) to the plaintiff's agents. Other requests were denied for a variety of reasons, including information system security, staff safety (a genuine threat), and third-party vendor non-disclosure agreements. Instead, the IEBC delivered highly sensitive information in "classified and sealed" form directly to the Supreme Court "for reference."[73]

In its final judgment, the ScoK comprehensively dismissed the allegations regarding a compromise of IEBC's RMS – "No credible evidence was presented to prove that anyone accesses the RTS (Results Transmission System) to intercept, detain or store [results] before they were uploaded onto the Public Portal."[74] Furthermore, such irregularities and technology failures that did occur were "not of such magnitude as to affect the final result of the presidential election." The ScoK upheld the results of the election – a legal victory for the embattled EMB. It is clear from the summary, and the subsequent full judgment, that IEBC's response to scrutiny in 2022 was aimed at demonstrating that its results management systems were not compromised and that the final result of the Presidential Election could be independently verified.[75] Despite their successfully defending the 2022 Presidential Election in the ScoK, IEBC was criticized[76] for failing to adequately communicate with electoral stakeholders about the various technologies used in its management

---

[72] *See* https://electionjudgments.org/en/entity/lmwns6vs8z?searchTerm=scrutiny&page=4 for an elaboration of the term "order for scrutiny" in the context of Kenyan electoral dispute resolution.

[73] Chief Registrar of The Judiciary Supreme Court of Kenya. (2022, September 2). *Registrar's ICT Scrutiny, Inspection, Scrutiny and Recount Report*. Final Report. https://www.judiciary.go.ke/?wpdmpro=final-registrars-ict-scrutiny-inspection-scrutiny-and-recount-report

[74] Supreme Court of Kenya. (2022, September 26). Presidential Election Petition No. E005 Of 2022 – Full Judgment. (par. 108). https://www.judiciary.go.ke/presidential-election-petition-2022/

[75] NATION. (2022, September 25). *Read: Supreme Court judges' presidential petition verdict in full, why Raila.* https://nation.africa/kenya/news/read-supreme-court-judges-full-judgment-on-raila-petition-3962334

[76] For example, see the European Union Election Observation Mission to Kenya 2022. *Final Report.* (p. 15). https://www.eods.eu/library/EU_EOM_Kenya_2022_EN.pdf

of elections. Allegations will inevitably arise in such a vacuum. In 2017, they stuck and in 2022, they did not.[77]

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 RMS – 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…"[78] Such support is complementary to other forms of technical assistance, enabling USAID partners to promote credible election processes while also preventing cybersecurity breaches.

Given the importance of transparency and accountability in the counting, aggregation, transmission, and publication of election results, programming should focus on encouraging and facilitating EMBs to fully embrace both principles in their design and implementation of RMS.

The legal framework for the management of results should be unambiguous without tying the EMB's hands by being too explicit on technologies. Technical assistance to educate and inform legislatures is one way that could help ensure such structures are codified. Support to electoral stakeholders should build a more detailed understanding of RMS and the security and process requirements needed at each stage of the process. To enhance transparency, support can also be provided for independent, parallel verification of the results from polling stations to final aggregated results.[79]

For programming that supports strengthening the RMS itself, consideration should be given to avoiding all-or-nothing technological solutions (where paper is abandoned) and favoring parallel paper/electronic results transmission. As our case studies have shown, trouble-free implementation of high-technology solutions across the electoral cycle in developing or post-conflict countries is rare and, when paper is absent, the price of failure can be very high indeed. An evolutionary approach (from all-paper to hybrid and, if eventually desired, paper-free solutions over multiple electoral cycles) is prudent.

Where programming is in support of national or institutional cybersecurity reform and capacity building, it may be important to ensure that EMBs are included explicitly in the mix of planned technical assistance. This is due, in part, to the need for the EMB to remain in control of electoral processes – including any activities in the cybersecurity context – where other agencies, possibly reporting directly to elected leaders or led by politically-appointed officials – are involved.

---

[77] For more on the Kenya presidential election petitions, please *see* https://www.ifes.org/publications/ifes-election-case-law-analysis-series-lessons-use-technology-elections

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

[79] For example, where appropriate, a parallel vote tabulation (PVT) conducted by nonpartisan citizen (domestic) election observers can independently verify the accuracy of election results. For more details, *see* USAID's Assessing and Verifying Election Results (2015). https://pdf.usaid.gov/pdf_docs/PA00KGWV.pdf

USAID Missions, other development agencies, and implementing partners can support stakeholders with a range of programs to help facilitate and maintain cybersecurity across key RMS phases – the capture, storage, transmission, verification, and publication of election results. The strategy outlined in *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."[80]

USAID and other development agencies can:

- **Support the development and implementation of cybersecurity assessments based on global best practices and as outlined above.** The first step in addressing cybersecurity when supporting programming for RMS 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 RMS that require the greatest attention.

- **Support relevant stakeholders, including EMBs and legislators, to integrate good cyber practices into RMS.** For example, this could include establishing policies and regulations concerning the storage and transmission of results data to include minimum encryption, physical and electronic security standards. This includes providing assistance when countries are transitioning between all-paper, hybrid, and fully-automated RMS to avoid missteps like those outlined above.

- **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 procurement, implementation, operation, sustainment and upgrading, and finally decommissioning and disposal. Doing so ensures 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 RMS 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 learning, especially as new technology, software, and cyber threats emerge in the election space.

- **Where appropriate, assist EMBs in cost-effective and transparent procurement and investment of secure results management technology and infrastructure.** For example, RMS may increasingly use mobile providers, VPN, and "cloud services" to store and process results information. To the extent that third-party service providers are employed, EMBs can be

[80] Ibid.

supported with technical assistance to ensure that 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 RMS, there are multiple constituencies, including government officials, EMB staff members, and others responsible for implementation of results management steps. Through training, technical assistance, and capacity building for both general cybersecurity practices and secure results management processes, the relevant stakeholders will be better equipped to adopt and implement proper cybersecurity procedures throughout every step. The introduction of basic cyber hygiene training focused on individuals with access to sensitive data, such as polling staff and personnel at tallying centers, can help prevent techniques such as phishing, as users are prepared to recognize and mitigate them. Further technical assistance tailored to the specific results management 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 analyses, programmatic support, and cybersecurity auditing and technical testing.

- **Promote and support training and technical assistance for EMBs to protect their staff from intimidation and coercion** and to implement early-warning systems to facilitate appropriate responses.

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

- **Support EMB's strategic communications capacities around cybersecurity and incident responses.** A critical part of this support would be to improve EMB's capacities in the area of strategic communications around cybersecurity and results management processes, particularly when an incident response is ongoing. Independent of any incident, EMBs can help build trust in RMS, and the larger election system through proactive and strategic engagement. This type of engagement can bolster resilience after an incident and mitigate disinformation that tries to harness real or invented cyber vulnerabilities.