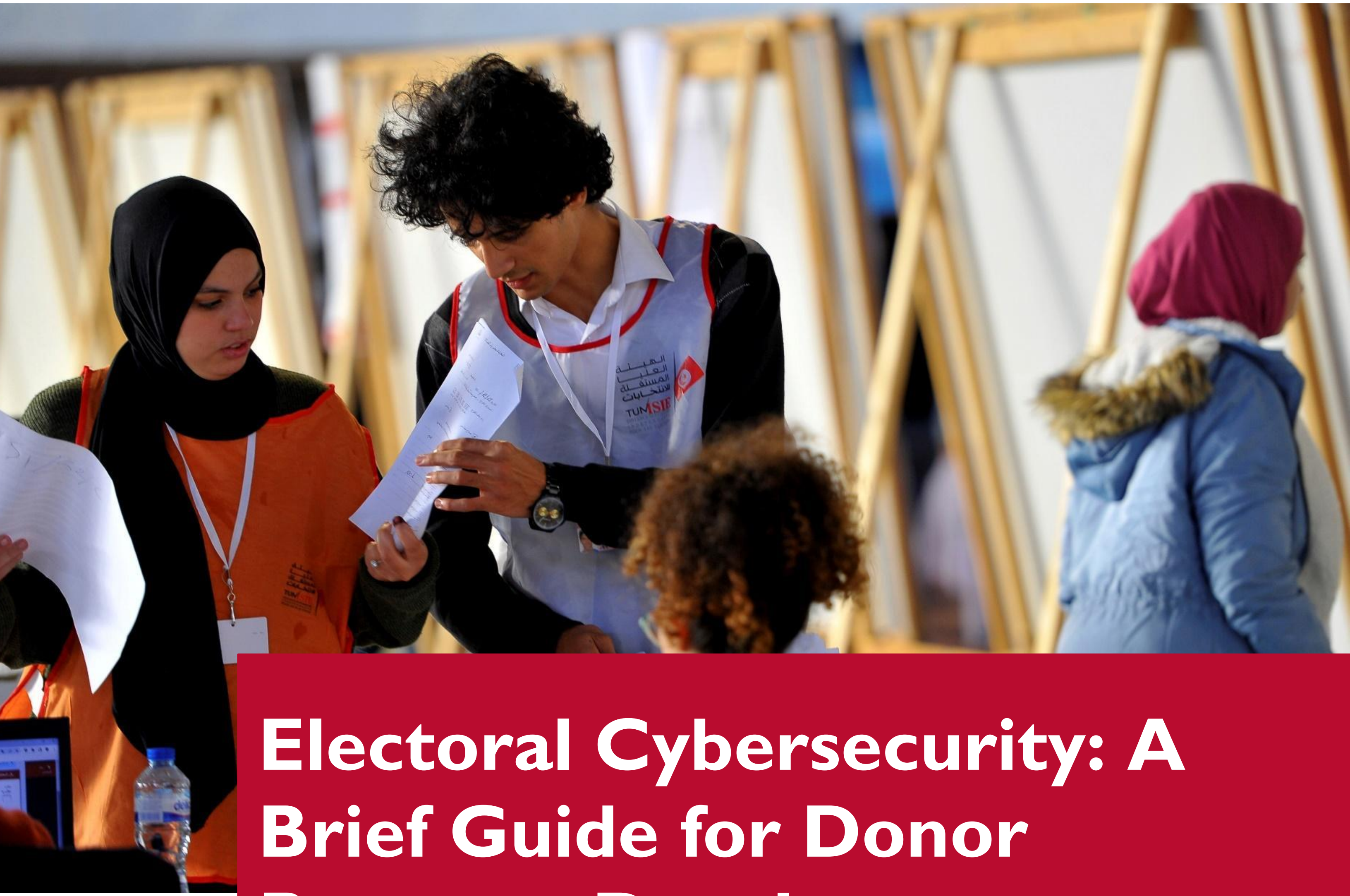


Vote counting in Tunisia, 2018
AP Photo/Yassine Mahjoub/NurPhoto.

Electoral Cybersecurity: A Brief Guide for Donor Program Development

February 2023

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). Mike Yard, Veronika Prochko, and Dr. Tarun Chaudhary are the lead authors. The paper benefited tremendously from contributions by Erica Shein and Matt Bailey. 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: Executive Summary

Election integrity is a critical element for democracy. Without secure, safe, and effective elections, democracy and its institutions are unable to flourish, threats to peaceful transition can emerge, and progress towards civil rights can be derailed. The way an election is managed shapes public perception, both among citizens and the world stage. International assistance for electoral processes helps strengthen and protect electoral integrity through capacity building, risk assessments, legal framework and dispute resolution mechanisms, training, and other assistance activities. Nevertheless, elections are rapidly leveraging new and old technologies within elections, such that technology and cybersecurity now play a central role in ensuring electoral integrity.

CYBERSECURITY

Cybersecurity, in this instance, refers to how electronically processed information is secured against disruption, disablement, destruction, or malicious control, thus protecting its confidentiality, integrity, and availability.

Elections have become a target for malign actors who want to undermine and disrupt a core democratic process. Despite the importance, cybersecurity programming is an often-overlooked component of international assistance due to the sensitivity of the topic to Election Management Bodies (EMBs) and host governments, and due to how opaque the field of cybersecurity is, often viewed as the exclusive domain of specialists. As election managers and stakeholders embrace technology solutions and electronic data, it is increasingly important that international assistance encourage and support cybersecurity programming. This prioritization is critical as cybersecurity threats have outpaced the sophistication of EMB cybersecurity defenses. Electoral programming of any type should consider including a cybersecurity component or add-on to strengthen the impact and scope of the program, since information technology is integrated recurrently across various aspects of election management. Cybersecurity programming should utilize the lenses of people, policy, and technology approach to identifying solutions for managing electoral cybersecurity risks. Successful and responsive cybersecurity programming should include activities that build, enable, or strengthen cybersecurity risk management, sound regulatory frameworks, institutional strategies with well-defined processes and procedures, comprehensive communication strategies for crisis and public relations management, and regional and international networks for electoral cybersecurity. These activities and approaches empower host countries to soundly protect their elections, especially as technology and cybersecurity begin to touch nearly all aspects of the election process.

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 personnel, USAID implementing partners, and local electoral stakeholders, on cybersecurity issues and program development recommendations. The paper first discusses the context within which cybersecurity programming is necessary in section II. Section III presents a four-step process to assess context and threat environment, identify and understand important EMB institutional partners, assess EMB cybersecurity capacity, and finally determine the level of openness to cybersecurity programming assistance within an EMB. Section IV explores various types of cybersecurity programming, followed by Section V with conclusions and recommendations.

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*,[1] *Understanding Cybersecurity throughout the Electoral Process: A Reference Document*,[2] and *Briefing Paper: Cybersecurity and Voter Registration*,[3] and *Briefing Paper: Cybersecurity and Results Management Systems*.[4]

[1] Chaudhary, T. (2022 July). *Primer: Cybersecurity and Elections*. USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf

[2] Chaudhary, T., Chanussot, T., and Wally, M. (2022, September 16). *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document*. USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK5H.pdf

[3] Chanussot, T. and Chaudhary, T. (2022 July). *Briefing Paper: Cybersecurity and Voter Registration*. USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK6G.pdf

[4] McDermott, R., Prochko, V., and Chaudhary, T. (2023, February 28). *Briefing Paper: Cybersecurity of Election Results Management Systems*. USAID, DAI, and IFES publication. https://www.usaid.gov/sites/default/files/2023-05/Briefing_paper_2_Election_Results_Management.pdf

Section II: Context

Cyber attacks against public institutions – including those aimed at election infrastructure – are occurring with increasing frequency globally.[5] Malign actors, whether foreign or domestic, use technology to enhance their reach and the damage they can inflict. Yet as cyber attacks become more frequent, electoral processes are more reliant on the kinds of technology those attacks exploit. Elections increasingly depend on technology such as digital voter rolls and election results, biometric voter registration, and electronic voting machines.[6] The public is generally aware that cyber attacks are likely, and many doubt – often with good reason – that their countries are prepared to successfully counter them.[7] As technology changes, EMBs and their partners must adapt their security to address and anticipate evolving threats. Although there is a growing body of materials addressing policy, principle, and practice in electoral cybersecurity, the unfortunate reality is that there are also an increasing number of cyber threats confronting election managers. These include well-funded foreign state actors and domestic actors, all with an interest in disrupting electoral processes and creating a narrative that sows public distrust in the credibility of elections.

Even with the growing threats posed by technology and avenues through which threat actors can attack elections, EMBs are often reticent to talk about cybersecurity because of the sensitivity of the topic. This makes it challenging for donors and implementing partners to assess the need for cyber electoral assistance. It is clear, however, that elections must be inclusive, accountable, transparent, and ***secure*** to support sound democracy; therefore, ensuring the cybersecurity of elections is a priority. Technical assistance focused on cybersecurity of elections can be provided in stand-alone programs or integrated into other assistance programs. This brief guide aims to assist USAID Democracy, Human Rights, and Governance (DRG) staff, other relevant U.S. Government personnel, the wider electoral assistance

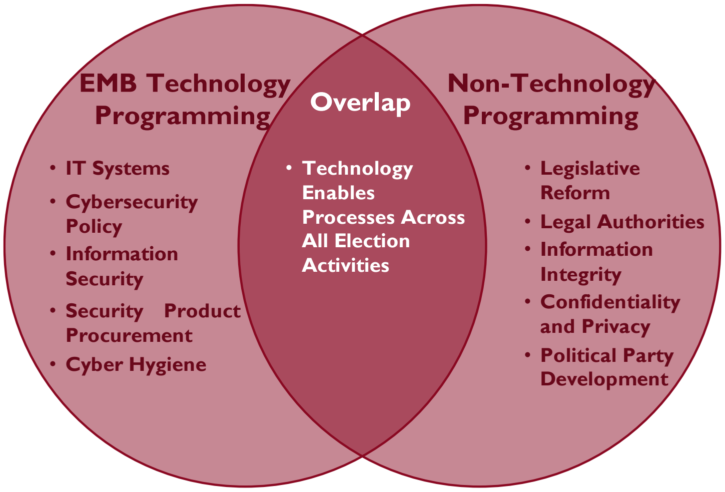
[5] For example, attacks targeted Colombia's voter registration system in advance of 2018 elections, Arostegui, Martin (2018, March 15). *Colombia Probes Voter Registration Cyberattacks Traced to Russia's Allies.* Voice of America. https://www.voanews.com/a/colombia-voter-registration-cyberattacks-russia-allies/4300571.html; In the Asia-Pacific region, election bodies and government agencies have been targeted with phishing and water holing operations. See Lim, Y. (2020, November 22). *Election Cyber Threats in the Asia-Pacific Region*. Mandiant. https://www.fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html; It is also useful to review US incidents such as: Turak, Natash. (2020, October 31). *Iranian hackers are targeting state election websites and accessing voter data, FBI says.* CNBC. https://www.cnbc.com/2020/10/31/fbi-iranian-hackers-are-targeting-state-election-websites-voter-data.html; In 2016, Ghana's election commission experienced a hack that reportedly attempted to post fake results to the website: *Ghana election commission website hit by cyber attack*. (2016, December 8). BBC. https://www.bbc.com/news/world-africa-38247987; In addition, botnets were leveraged to spread mis- and dis-information around Mexican elections. See Marañon, A. (2021, May 28). *How Have Information Operations Affected the Integrity of Democratic Elections in Latin America?* Lawfare. https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democratic-elections-latin-america; US elections have been targeted by cyber attacks, as have Australian political parties and the federal parliament. See Galloway, Anthony. (2020, Oct 28). *Cyber Attacks on Elections Growing Amid Concern for Australia's Political Parties*. Sydney Morning Herald. https://www.smh.com.au/politics/federal/cyber_attacks-on-elections-growing-amid-concern-for-australia-s-political-parties-20201028-p569fg.html

[6] K. Ellena et al. (2018). *Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies*. IFES. https://www.ifes.org/publications/cybersecurity-elections

[7] The Pew Research Center surveyed 26 countries from regions across the world about their expectations for cyber attacks in elections. Learn more at Poushter, J. and Fetterolf, J. (2019, January 9). *International Public Braces for Cyberattacks on Elections*, Infrastructure, National Security. Pew Research Center.

community, and local stakeholders in assessing cybersecurity needs related to the electoral environment and prioritizing assistance to help EMBs address the most significant cyber threats they face.

A. The Need for Consistently Integrating Cybersecurity


EMB Technology Programming
• IT Systems
• Cybersecurity Policy
• Information Security
• Security Product Procurement
• Cyber Hygiene
Overlap
• Technology Enables Processes Across All Election Activities
Non-Technology Programming
• Legislative Reform
• Legal Authorities
• Information Integrity
• Confidentiality and Privacy
• Political Party Development

Examples of overlap between technology or cyber-focused programming and seemingly non-technological programming

Technical assistance to elections touches many aspects of election management and, therefore, many institutions. Direct support to EMBs may address general issues (for example, advising on legal frameworks, helping to create strategic plans, guiding policy on technology implementation), or it may address specific election cycle activities such as voter registration, voter education, political party and candidate registration, ballot production, and results transmission. Many actors beyond the EMB are also touched by international assistance, including government ministries, legislative bodies, the judiciary, security forces, political parties, and civil society organizations.

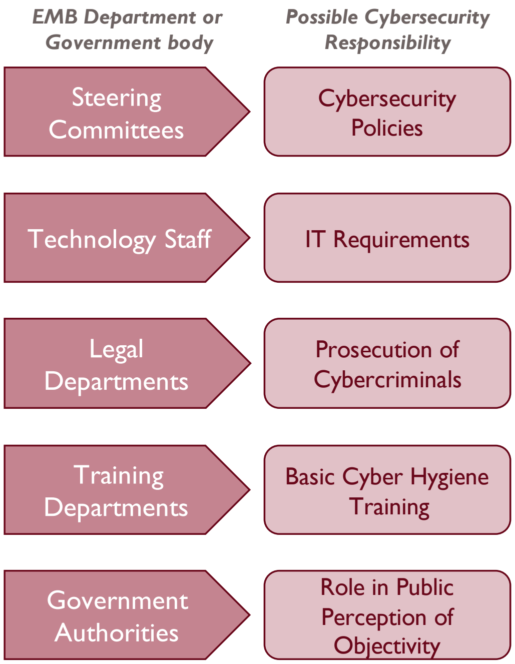
Although there is clear value to stand-alone projects that focus on cybersecurity, it is also necessary to address cyber threats when designing other election assistance activities. There is some risk of exposure to cyber threats in almost every aspect of the electoral cycle; therefore, every election assistance project where technology is involved in any way should include a cybersecurity component. At a minimum, each project should assess the potential for new vulnerabilities or threats that may be introduced through the activity. Additionally, whenever possible, projects should work to identify existing threats that may impact the project and further enhance protections in the departments and/or institutions served.

For example, the election commission appointment process at subnational levels is often an important issue in many countries.[8] An assistance activity might seek to help identify and evaluate different approaches to the appointment process. The overall purpose would be to improve the process, ensuring that candidates for regional and local commissions have requisite knowledge and skills and that the commissions are either nonpartisan or politically balanced. On the surface, it might not seem like this activity would call for a cybersecurity component. However, it would be worthwhile to include a minor cybersecurity component to address the risk of unauthorized access or alteration of candidate forms as

[8] An example of a missed opportunity to provide comparative analysis to an EMB that included a cybersecurity component can be seen in a study conducted by the International Foundation for Electoral Systems (IFES) in 2020 in North Macedonia. IFES provided comparative examples to the EMB of commissioner appointment processes at the subnational levels in several different countries. The study analyzed the strengths and weaknesses of the different appointment mechanisms but, due to the limited scope of the project, did not address the cybersecurity risks of appointing untrained persons and giving them access to the CEC WAN. This was a missed opportunity as the analysis could have been strengthened by a consideration of the cybersecurity concerns to a seemingly non-technological study.

they are transmitted through the entire process, from candidate to political party (where relevant) to the central EMB, as they are stored on the EMB's servers, and as they are reviewed by the body designated to evaluate candidates. A malign actor could make slight alterations to applicants' forms at any of these points, corrupting the appointment process. Therefore, the technical assistance should include an evaluation of the level of risk related to the process to build in safeguards. For more thorough assistance, the cybersecurity component could also identify the cyber hygiene training needs of newly-appointed regional or local commissioners and provide them with the knowledge and practices to safeguard the commission offices from cyber threats.

B. The Need for Holistic Engagement



EMB Department or Government body	*Possible Cybersecurity Responsibility*
Steering Committees	Cybersecurity Policies
Technology Staff	IT Requirements
Legal Departments	Prosecution of Cybercriminals
Training Departments	Basic Cyber Hygiene Training
Government Authorities	Role in Public Perception of Objectivity

Cybersecurity is an important development priority; to obtain sustainable development outcomes, it should be approached holistically throughout the phases of planning, delivering, assessing, and programming adaptation. This guide can be used in conjunction with the process outlined in *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.*[9]

Many electoral assistance activities only require interaction with specific departments within the EMB. A program implementing a voter education activity may only need to build a relationship with the voter education department, for example. And voter registration projects typically only require interaction with voter registration and technology staff.

Cybersecurity interventions, on the other hand, require a broader and deeper level of involvement from the EMB, and possibly from other government ministries and agencies involved in cybersecurity. Commissioners must understand the types of threats and the consequences of attacks on different types of information assets. Steering committees drafting policies related to cybersecurity within EMBs often include at least one commissioner, some upper-level management, and key operations staff. Technology staff must understand how to install and maintain security hardware and implement policies to control and monitor the types of devices and software that are allowed to have access to the network. They must also know how to tailor cybersecurity standard practices to electoral technology, which is often bespoke and lacks robust, integrated cybersecurity measures. Legal departments must be familiar with laws designed to deter cyber attacks and prosecute cyber criminals. Training departments may be required to create basic cyber hygiene training programs and to define strategies for keeping staff up to date on best practices to protect against cyber threats. Government authorities involved in investigating a cyber attack may need orientation to understand how their role must be clearly defined to avoid perceptions that they are interfering in electoral matters.

[9] Byers, S. and Nurko, G. (2021 October). *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.* DAI and USAID publication. https://www.usaid.gov/digital-development/usaid-cybersecurity-primer

In the past, initial attempts to address electoral cybersecurity focused on building the capacity of the EMB's technology department, but over the past decade, it has become clear that cybersecurity is an issue that must be addressed by the entire EMB and its partner organizations. This holistic engagement across departments, institutions, and organizations is important for assistance design, as the donor may want to map out the relevant actors to ensure consistent and broad engagement. This kind of approach can limit duplicative programming or gaps in programming and can assist in strengthening the electoral cycle more efficiently. Nevertheless, it is important to keep in mind that in some countries, cooperation and communication between different government institutions around elections can be challenging. Despite this, assistance that engages with all the relevant stakeholders contributes to the long-term improvement of electoral processes across the EMB and other government institutions.

C. Electoral Assistance Challenges

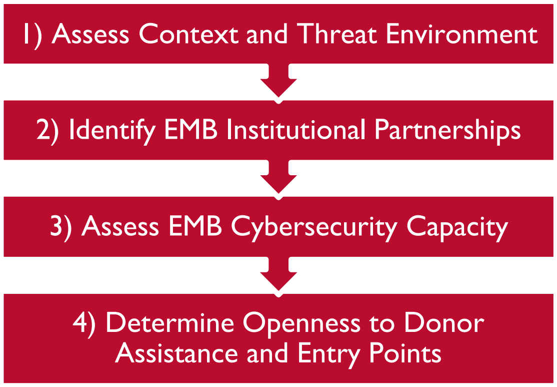
More technology and the accompanying cyber threats bring significant challenges for electoral assistance programs. First, the increased use of technology in elections comes with increased cyber risk, from the obvious cases of biometric voter registration and electronic voting to the less visible processes such as party and candidate registration, communication between election managers, and ballot production. Secondly, the internet's rapid global expansion has made the electoral process an attractive target for both international and domestic actors wishing to destabilize a country or damage the credibility of its elections. The easy accessibility of malware components and Cybercrime as a Service (CaaS)[10] has made conducting cyber attacks cheaper, putting powerful tools in the hands of a growing array of malign actors.

Unfortunately, it is not only actual cyber breaches that create problems for elections; even the *perception* of vulnerability of election systems can undermine voter confidence. EMBs' sensitivities about public perception around an election can make them hesitant to engage with international assistance, not wanting to be seen as enabling or inviting "foreign interference" or influence into the process. In addition, EMB staff often do not have the required cybersecurity expertise. Consequently, international assistance may want to consider integrating cybersecurity into their other programing to work around this reticence. Additionally, as mentioned previously, holistic approach towards cybersecurity in international assistance may lessen the unwanted attention or spotlight an EMB may feel if international assistance were to only engage with it on cybersecurity rather than across all stakeholders involved in elections.

[10] Cybercrime as a Service (CaaS) refers to the sale of expertise and resources by cyber-criminal groups for profit. Criminal groups will, for example, "rent" their command and control of infected computers to direct requests that, through request overload, cause servers to crash.

Section III: Assessing Electoral Cybersecurity Needs

Four Steps to Assess Cybersecurity Needs


1) Assess Context and Threat Environment

2) Identify EMB Institutional Partnerships

3) Assess EMB Cybersecurity Capacity

4) Determine Openness to Donor Assistance and Entry Points

Electoral assistance programs should always be informed by a prior assessment of the electoral cybersecurity context of the country or locality. Given the significant variation in cybersecurity capability, **capacity, risk tolerance, and threat environment, the** assessment phase is crucial. This context assessment may be incorporated into a broader electoral assessment conducted or supported by the donor, or it may be delegated to third parties such as international non-governmental organizations, contractors, or consultants. The following four-step process is designed to help drive understanding.

Step 1: Assess Context and Threat Environment

Key Elements:

- Political Landscape
- Socio-Economic Factors
- Historical and International Context
- Public Confidence
- Electoral Context
- Threat Actors

1.1 Analyzing the Bigger Picture

Before assessing the cyber needs and vulnerabilities of a particular country's election framework, a donor should begin by assessing the country context and threat environment. Not all elections may attract the same level of attention from foreign or domestic cyber attackers. Motivations for an attack differ according to whether the country has a major impact on world events, is experiencing tensions or open conflict with a neighboring state, or has highly volatile internal politics. To assess the context, relevant political, social, and economic factors that may impact the election and create opportunities for cyber threats must be considered. For example, the levels of digital literacy and economic well-being of a population, historic or cultural distrust of political institutions, or socio-economic or political divisions among citizens should be factored into the cybersecurity threat landscape. This assessment may include some or all of the following aspects:

- Understanding the regime type, political system, and the country's overall level of adherence to democratic principles and electoral independence.

- Understanding the political landscape, including identifying key political players and parties, political platforms, and key issues, and whether there are significant ideological or ethnic divisions reflected in the political processes.

- Analyzing the social and economic factors such as demographics, economic conditions, political finance, and any divisive social issues that may affect voter sentiment and behavior. What vulnerabilities and sensitive issues could a threat actor manipulate?

- Reviewing the political and historical context, including whether past elections have been perceived as credible, whether there were post-election conflicts, and the degree to which a governing party(ies) controls access to national resources. How does this affect the way election disputes are handled or the probability of elections being overturned in the face of scrutiny?

- Monitoring media coverage, particularly whether there are significant biases among outlets, potential misinformation, and/or hate speech in social media. How can the narrative surrounding an election be misconstrued? How can a minor issue picked up by the media expand beyond the EMBs control?

- Analyzing the international context surrounding the election, any potential impact on foreign governments, key out-of-country political influencers, and animosity of neighboring states known to actively engage in cyber attacks related to elections.

- Understanding the level of public confidence in the EMB and judiciary, as well as any other institutions that may play a key role in elections. How difficult would it be to erode trust in the electoral systems using an actual or alleged cyber attack?

There are a number of means by which the donor can approach answering these, including using USAID-developed tools to assist with this analysis, like the Digital Ecosystem Country Assessment (DECA) and the DECA Toolkit:

DIGITAL ECOSYSTEM COUNTRY ASSESSMENTS (DECA) TOOLKIT

The DECA is organized around USAID's Digital Ecosystem Framework, which includes three research pillars: digital infrastructure and adoption; digital society, rights, and governance, and digital economy. As elements of the digital ecosystem are innately interdependent, there are four cross-cutting topics, one of which is cybersecurity. The DECA includes topics such as the existence of cybersecurity policy, regulation, and standards; government processes and capacity to address cyber threats; the safety of critical internet infrastructure, institutional response plans to cyber breaches; and individual level understanding of and protection against cyber threats. More in depth information on how a DECA researches cybersecurity can be found in the DECA Research Checklist. The DECA Toolkit provides a step-by-step guide on how USAID Missions can hire and manage research teams to independently conduct a DECA. Additional details and publicly available DECAs can be found here.

1.2 Narrowing in on the Electoral Framework

Following DECA or other country context assessments, the donor should then consider these factors within the context of the country's election framework. An electoral assessment should consider how the country's elections are conducted and to what extent the country context affects election administration. USAID's *Electoral Assessment Framework* is a useful framework for this analysis.[11] It provides a process

[11] Ivantcheva, A., McNulty, M., Sahley, C., and Seats, E. (2021 March). *Electoral Assessment Framework A Tool to Assess Needs, Define Objectives, and Identify Program Options*. USAID. https://pdf.usaid.gov/pdf_docs/PA00XCC2.pdf. See also,

through which a donor can identify and prioritize the various electoral integrity challenges within a specific country and how those challenges can affect the election process and the EMBs responsible for administering them. Implementing partners can also be utilized and may offer useful tools and methodologies to give donors a comprehensive understanding of a country's electoral system.[12]

Following this assessment, the donor should seek to identify potential attackers and threats. As more countries digitize their electoral processes, they may be exposing more of their electoral infrastructure to risks, creating potential vulnerabilities to threat actors. Understanding which risks need to be prioritized for a given EMB or electoral environment is key. Cyber risks can be further compounded by poor cyber hygiene among institutions, and users involved in administering and maintaining election technology can further compound cyber risks. Ad hoc and piecemeal approaches to cybersecurity involving third parties, technology procurement and multi-stakeholder collaboration can make holistic cybersecurity management difficult or impossible.

Identifying risks requires understanding what kinds of threats exist, how vulnerable data and infrastructure may be to those threats, and importantly, the consequence of a particular threat playing out. The risk-graded approach detailed in *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming* can be utilized to help drive cybersecurity priorities, specifically: "Missions can systematically identify, understand, and prioritize the cyber vulnerabilities and threats within partner countries and work with the governments to prioritize actions and resources to address them."[13] More detailed information regarding how to understand and categorize risk can be found in *Primer: Cybersecurity and Elections*.[14]

1.3 Understanding Motives

When utilizing a risk-based approach to assess the cyber threats to a host country's election, the donor must consider both domestic and international actors and their potential motivations. Is there significant cyber-crime in the country? Is the country a likely target for foreign state-funded interference, particularly from the People's Republic of China (PRC), Russia, North Korea, or others motivated to influence the country's government or to undermine democracy? Threat actors may have a range of motives, from mischief to malice to manipulation. Some actors may look to manipulate the results of an election, while others seek to undermine the credibility of the electoral process in general or to erode trust in democracy. There are well-known motivations of past cyber attacks on elections launched by well-

Fischer, J. Kaplan, K., and Bond, E. (2010 July). *Electoral Security Framework: Technical Guidance Handbook for Democracy and Governance Officers*. USAID. https://2012-2017.usaid.gov/sites/default/files/documents/1866/1-Electoral-Security-Framework.pdf

[12] IFES offers a comprehensive Electoral Integrity Assessment for mapping vulnerabilities throughout the electoral process, providing a blueprint for democratic resilience. Using the tool, IFES analyzes vulnerabilities to systemic manipulation, malpractice, and fraud across 18 different areas of the electoral process. The assessment can then be used to create plans to address identified gaps. The full assessments are not publicly shared, but an example public summary can be found here: https://www.ifes.org/publications/mali-electoral-integrity-assessment

[13] Byers, S. and Nurko, G. (2021 October). *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.* DAI and USAID publication. (p. 21). https://www.usaid.gov/digital-development/usaid-cybersecurity-primer

[14] Chaudhary, T. (2022 July). *Primer: Cybersecurity and Elections.* USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf

resourced foreign state actors aimed at undermining trust in democratic processes and the legitimacy of their outcomes.[15]

Domestic cyber attacks can also inflict similar damage to an election. Domestic actors may be politically, financially, or ideologically motivated, or may seek to exacerbate tensions for a variety of reasons. They may operate individually or collectively. Like their foreign counterparts, they often seek to create tensions and sow mistrust in elections and democratic institutions. The various threat actors and entities can be categorized as follows:[16]

1. **Foreign State Actors and Advanced Persistent Threats -** Malicious actors associated with or directly tied to foreign governments. This category of threat actor is generally well-resourced and utilizes sophisticated techniques. The term "Advanced Persistent Threat", or APT, is used to describe this level of sophistication.

2. **Government Actors -** Government actors often work against certain electoral stakeholders within their own state, particularly in countries that are electoral autocracies or have characteristics of this typology. Their efforts aim to discredit and hamper the operation of certain political or civil society actors. Government actors can also make use of their own means of surveillance to pressure, intimidate, expose damaging private information, or prosecute electoral stakeholders seen as problematic or contrary to the interests of political actors in control of state resources.

3. **Criminal Groups – Cybercrime-as-a-Service** – Criminal groups are often involved in cybercrime for financial gain (for instance, ransomware attacks against state and local institutions). There is little official record of EMBs paying a ransom to recover data, and it seems that in most cases, election-related victims were collateral damage from larger attacks on government infrastructure. However, criminal groups have targeted electoral infrastructure and, as a tactic, it could become more widespread. The willingness of cyber criminal groups to "sell" their expertise and resources has given rise to the term Cybercrime as a Service (CaaS).

4. **Non-State Political Groups and Hacktivists** – Criminal activity of non-state political groups (including political parties and candidates) and activist individuals can also target election-related infrastructure and other parties, candidates, or related (e.g., fundraising, and political) organizations. Hacktivism is a term used to describe the blending of hacking and activism regarding political and social issues. This type of activity can be organized and domestically based and can be driven by transnational collaborators or individuals. In addition, there are examples of foreign

[15] For a useful summary of Russian activity see: Tennis, Maggie. (2020, July 20). *Russia Ramps up Global Elections Interference: Lessons for the United States*. Center for Strategic & International Studies. https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states; see also BBC. (2020, September 11). *Russia, China and Iran Hackers target Trump and Biden, Microsoft says.* https://www.bbc.com/news/world-us-canada-54110457; China is also active in this area, in the context of Taiwanese elections see: Sharp, Andrew (2018, November 28). *Beijing likely meddled in Taiwan elections, US cybersecurity firm says*. Nikkei Asia. https://asia.nikkei.com/Politics/Beijing-likely-meddled-in-Taiwan-elections-US-cybersecurity-firm-says

[16] For further elaboration about each category, see Chaudhary, T. (2022 July). *Primer: Cybersecurity and Elections.* USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf.

governments hiring hackers outside of their borders to carry out attacks on their behalf, blending the category of foreign state actors and non-state groups.

5. **Insider Threats** – Individual or collective threat actors might also operate from within EMBs. The motivations of insiders that decide to act against the interests of an EMB employer are poorly understood and therefore difficult to detect or address. However, a key component of any comprehensive cybersecurity program is to assess the threat of– and put controls in place against – insider threat mitigation.

1.4 What Exists Already?

Once a donor understands the country context, electoral context, and threat environment for a specific country, the donor should then turn to the national cybersecurity strategy in place. There are wide variations from country to country in legal and organizational structures related to cybersecurity. While most countries have developed national cybersecurity strategies, they vary in effectiveness and in the way they are structured. The National Cyber Security Index (NCSI) developed by the e-Governance Academy in Estonia is one of several ongoing projects that attempt to rank each country's cybersecurity strategy. The NCSI is updated regularly and focuses on four "measurable aspects of cyber security implemented by the central government:" [17]

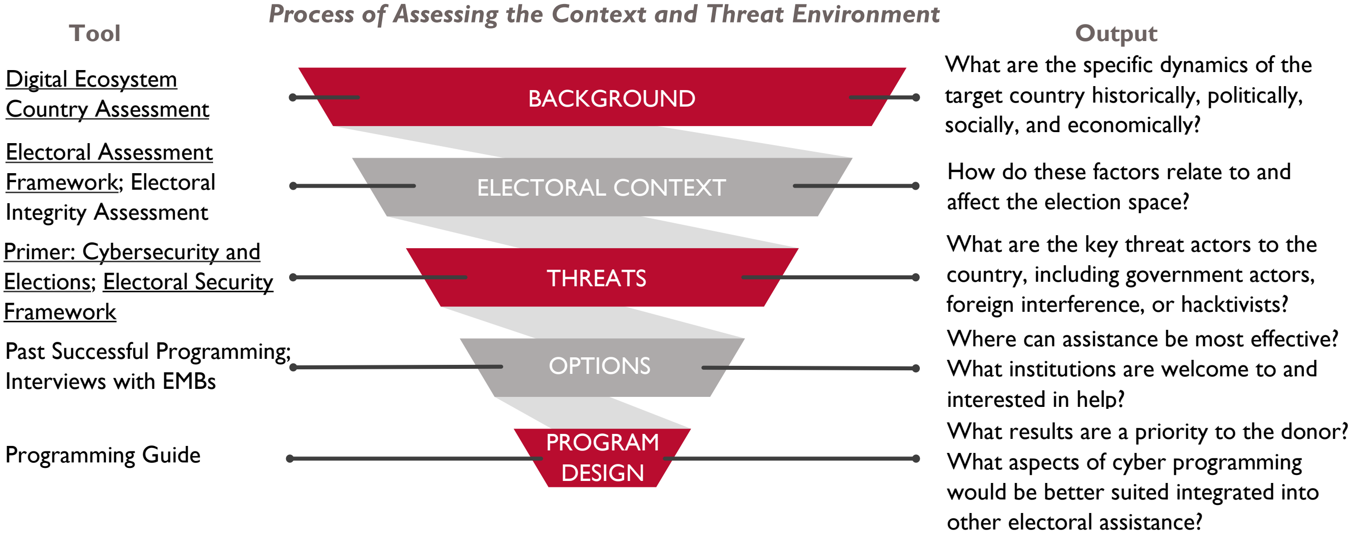
1. Legislation in force – for example, legal acts, regulations, or orders
2. Established units – for example, the existing organizations that are relevant and departments that have cybersecurity responsibilities
3. Cooperation formats – for example, committees, working groups, and other major cooperative initiatives
4. Outcomes – policies, exercises, technologies, websites, programs, and other outcomes that help serve as empiric measures of cybersecurity capacity and integration

The NCSI provides a convenient starting point for assessing the cybersecurity environment in a country. Analysis of the NCSI's detailed report for a country gives a concise picture of key indicators and may suggest priorities for strengthening either the national strategy or for assisting the EMB to define further safeguards to compensate for weaknesses in the national strategy. For more information, the International Telecommunications Union hosts a repository for National Cybersecurity Strategies that includes the approved or draft strategies from more than 100 countries.[18] National strategy documents are a useful starting point; however, the strategies may not be reflective of the holistic context, and often convey idealized or overly optimistic assessments of national capabilities that haven't actually been implemented yet, and are written without specific election-related information that is important to understand. Therefore, donors should view these resources as a starting point for assessing the overall cyber health of a country and with that, seek to better understand the election stakeholders, including the EMB and the EMB institutional partnerships.

[17] National Cyber Security Index. e-Governance Academy Foundation. https://ncsi.ega.ee (accessed 2023, January 19)

[18] International Telecommunication Union (ITU). National Cybersecurity Strategies Repository. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx (accessed 2023, January 22)

Process of Assessing the Context and Threat Environment



Tool		Output
Digital Ecosystem Country Assessment	BACKGROUND	What are the specific dynamics of the target country historically, politically, socially, and economically?
Electoral Assessment Framework; Electoral Integrity Assessment	ELECTORAL CONTEXT	How do these factors relate to and affect the election space?
Primer: Cybersecurity and Elections; Electoral Security Framework	THREATS	What are the key threat actors to the country, including government actors, foreign interference, or hacktivists?
Past Successful Programming; Interviews with EMBs	OPTIONS	Where can assistance be most effective? What institutions are welcome to and interested in help?
Programming Guide	PROGRAM DESIGN	What results are a priority to the donor? What aspects of cyber programming would be better suited integrated into other electoral assistance?

Step 2: Identify and Understand EMB Institutional Partnerships

Key Elements:
• Relationship Goals of EMB • Past Relationship Effectiveness • Relevant Organizations • Possible Partnerships

EMBs do not operate in a vacuum. Although EMBs are oftentimes defined within the constitution or legislation as independent bodies, they still operate within a complex set of relationships with public and private sector organizations and political and civil society stakeholders. Some EMBs have close ties to government departments or ministries (indeed, in some cases, elections are managed by a ministry or by a judicial body). Other EMBs may face antipathy from other government bodies, while still others must manage these relationships carefully because of public mistrust of the government's ability or will to maintain neutrality toward electoral processes. These political realities complicate what would otherwise be a straightforward technical issue – that is, to what extent can the EMB rely on other institutions to help create a robust cybersecurity infrastructure.

Analyzing EMB partnerships will help define strategies for responding to a cyber threat or a cyber attack. In particular, it is important to assess whether the EMB can expect a supportive, antagonistic, or neutral response from its partners in government and other necessary stakeholders. Cybersecurity can sometimes become a captured function of certain parts of a government, for example — national police or the ministry of defense may not respond well to EMB cybersecurity initiatives if they feel they challenge their authority on the subject. Understanding the dynamics around the receptiveness of potential EMB partners or entities that may become obstacles is important. An EMB must retain impartiality, which means that it must weigh whether and to what extent it should collaborate with other institutional partners. It is critical to understand the historical and legal context for EMB relationships and how it could affect the EMB's ability or desire to coordinate or collaborate with other government entities or civil society groups. Knowing and understanding nuanced relationships is necessary for program designers to formulate approaches for long-term strategy and the associated cybersecurity needs.

When analyzing key institutional partners, the donor should:

- Review the EMB strategic plan to understand its goals and communication practices in relation to government, political, and civil society stakeholders, including political parties and activist groups, the media, and the international community.

- Review observer reports from recent and previous elections to determine how effectively the EMB has engaged with its partners.

- Interview commissioners and senior staff who may have different perspectives on who the key partners are and the nature of the relationships with each partner.

- Identify organizations that play a role in the national cybersecurity strategy and determine the current level of cooperation between the EMB and those organizations. This includes mapping out the different relationships between the EMB and its partners, as well as the relationship these partners have with each other. Information exchange, level of cooperation, bureaucratic tendencies, and resource discrepancies are all important elements of this step. For example, if an EMB collects information for voter registration from a government ministry that maintains a national identity database, it is worth investigating whether the EMB and ministry have a Memorandum of Understanding (MoU) detailing the process for information exchange, reciprocal expectations of appropriate security, responsibilities for informing each respectively of breaches, and defined roles and responsibilities for incident response in the case the exchanged data is compromised or a connected system is breached.

- If appropriate, meet with both government and private cybersecurity organizations to explore openness to increased partnership with the EMB.

Step 3: Assess EMB Cybersecurity Capacity

KEY ELEMENTS:

- Existing Cybersecurity Framework
- Compliance Procedures
- Reviews for Controls and Updates
- Training Programs
- Intelligence Channels
- Incident Response Plans

As a donor, it is important to keep in mind that assessing the cybersecurity capacity of an EMB is not simply a preliminary exercise to determine whether cyber assistance is needed; rather, the activity may be seen as part of the programming necessary to understand and address existing gaps. It can also serve as the basis for further programming and subsequent assistance.

Assessing the EMB's cybersecurity capacity involves evaluating the organization's ability to protect its networks, systems, and data from cyber threats. Part of this assessment involves determining the cybersecurity maturity level. The concept of maturity is widely used in the cybersecurity community to refer to the ability and capacity of a cybersecurity program to help an organization identify, detect, deter, and respond to threats unique to its organization or field. Maturity models help organizations locate their baseline cybersecurity activity on a scale and identify what they would like to improve. Maturity indicators not only help to understand the programmatic and managerial characteristics of an organization's cybersecurity position, but they are also necessary to evaluate the cybersecurity workforce. The topic of maturity along with information regarding formal risk management frameworks can be found in the briefing *Understanding Cybersecurity Throughout the Electoral Process: A*

Reference Document.[19] The following list of example questions can help further build understanding of cybersecurity maturity within a specific EMB:

- Does the EMB have a clear existing cybersecurity framework (e.g., NIST,[20] ISO 27001,[21] COBIT[22]) or a clearly defined internal framework? To answer this question, and the ones below, the donor may need to request or support an implementing partner's or other third-party assessment of cybersecurity and technology for the EMB.

- Is there an institutionalized process for identifying, assessing, and prioritizing risks within the EMB?

- Does the EMB enforce compliance with relevant laws, regulations, and policies? If the donor identifies that it does not, it can request implementing partners formulate ways to help the EMB do so, whether through resource allocation, capacity building, or training.

- Does the EMB have a system in place to identify and manage critical assets such as technology devices, data centers, and communications channels?

- Are cybersecurity policies and practices reviewed? Is there a clear process for updating policies or recommending enhancements to security hardware and software?

- Is there a training system in place to acquaint employees with cybersecurity best practices and EMB policies?

- Does the EMB actively engage with and share intelligence with government and private cybersecurity organizations? With other EMBs in the region or internationally?

In addition to assessing the maturity level of the EMB, a capacity assessment should also:

- Review cybersecurity policy documents to determine if they are in line with best practices for public entities.

- Assess the effectiveness of the EMB's cybersecurity training program. Does it ensure that new employees are trained before accessing any technology? Have all existing employees been trained? Are there mechanisms in place for reminding employees of important cyber hygiene practices?

[19] Chaudhary, T., Chanussot, T., and Wally, M. (2022, September 16). *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document*: USAID, DAI, and IFES publication. https://pdf.usaid.gov/pdf_docs/PA00ZK5H.pdf

[20] National Institute of Standards and Technology (2020, December 10). *Security and Privacy Controls for Information Systems and Organizations.* SP800-53 Rev. 5. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[21] Joint Technical Committee ISO/IEC (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* ISO/IEC 27001:2022. International Organization for Standardization https://www.iso.org/isoiec-27001-information-security.html

[22] Information Systems Audit and Control Association (ISACA) (2019). COBIT. https://www.isaca.org/resources/cobit

- Understand the cybersecurity work roles in the EMB. What existing work roles are associated with information technology and cybersecurity? If those roles are blended across the two disciplines, it may also be useful to understand how IT and cybersecurity employees dedicate their time. Are there enough people to keep up with the demand for IT and cybersecurity services across the array of EMB activities, including both everyday EMB work and work dedicated to election technologies such as voting machines, biometric scanners, and others?

- Identify the state of the EMBs incident response plan, if one exists. Is it up-to-date and are key staff trained in how to respond in case of a cyber incident?

- Assess the EMB's current infrastructure, data controls, and inventory management. Does the EMB have an inventory of hardware and software assets under its management? Is there an understanding of what the data flows are across EMB-controlled infrastructure, and data flows between the EMB and other entities (government ministries, vendors/service providers, political parties and CSOs, etc.)? Has the EMB conducted penetration testing or vulnerability scanning to test the effectiveness of its security controls?

- Gauge the sophistication and competency of the EMB's security controls. Are there adequate controls such as security appliances, firewalls, intrusion detection systems, and antivirus programs? And are there adequate, qualified staff to configure and maintain them?

Step 4: Determine the Level of Openness to Donor Assistance and Identify Possible Entry Points

KEY ELEMENTS:

- Perception of Assistance
- Level of Political Bias
- EMB Priorities and Challenges
- Interview with Stakeholders

The recent history of international organizations' involvement in elections can give some indication of the country's openness to donor assistance, though a good deal can change during an electoral cycle. Donors should, in most cases, be able to anticipate the degree to which assistance will be welcomed, but there may be competing ideologies within the host government that impact how assistance will be perceived, and whether it will bolster or erode confidence in the integrity of the election. The contextual analysis gained from Step 1 should include knowledge of laws related to registration of international assistance providers, any history of politically-motivated attacks on domestic or international NGOs, or perceptions by the host country of political bias of the international community.

Identifying possible entry points for new technical assistance programs or activities focused on cybersecurity should begin with a review of past final reports or independent evaluations of past programs, international and domestic election observation mission reports, relevant legal petitions, and court responses. As mentioned previously, EMBs are often reluctant to discuss cybersecurity, even if they are open to other electoral assistance, due to how sensitive their internal security can be. With this in mind, and in particular if cybersecurity is not a current area of programming in the host country, the donor should consider holding interviews with commissioners, senior staff, and political and civil society representatives. These discussions may help the donor to gauge the level of openness to new or expanded assistance as well as build rapport that can provide windows of opportunity in the future. After this engagement, the donor can determine whether new or expanded direct cyber programming is necessary and possible. If the EMB is less open to cooperation, integrating cyber programming with other electoral assistance could help mitigate any concerns an EMB may have or fend off any real or perceived unwanted attention to the EMB.

In some cases, the donor may not have requisite expertise in legal frameworks, election operations, and technology to assess electoral cybersecurity challenges and needs, or the EMB may not be able to objectively assess its own performance. In such cases, it is advisable to consider bringing in a third party, such as an independent consultant or a technical assistance provider that can conduct the assessment and make programmatic recommendations.[23]

Leveraging a Systems Approach to Program Design

After completing the above steps to determine the level of need and types of cyber vulnerabilities in the host country, a donor has a comprehensive information source to integrate cybersecurity into development programming and assistance to an EMB. The donor can apply a "systems thinking approach" that situates cybersecurity within the larger context and mission of an EMB. The systems approach utilizes the people, processes, and technology conceptual lens:

- **People**: The people component examines capacity, behaviors, and resources needed for individuals to align their own work with the mission of the organization. In the cybersecurity context, this includes taking all the proper steps associated with cybersecurity and their work role. For a technical IT or cybersecurity specialist, this may include specialized training or direct IT/cybersecurity responsibilities. For other staff, this could include cyber hygiene training and application. Donor organizations can support each of these training types as one element of EMB cybersecurity capacity building.

- **Process**: Processes that are repeatable and feature institutionalized mechanisms for documentation, distribution, and inculcation are an important component of any well-functioning organization. In the cyber security context, this may include formalized, documented cybersecurity policies and processes that are periodically evaluated for effectiveness. Donor organizations can support EMBs with technical assistance to draft, implement, and institutionalize these policies and processes. They can also help EMBs audit their processes to make sure the policies are having the necessary effect.

- **Technology**: The "technology" component references the types of hardware, software, and other solutions that can be utilized to achieve desired effects and goals. Technology should not be thought of as a cure-all; whenever technology is leveraged, there are people and process implications, as outlined above. Additionally, when technology is integrated or being proposed for

[23] For example, IFES' methodology, Holistic Exposure and Adaption Testing (HEAT), provides a process through which an EMB can test its current cybersecurity practices, risk mitigation procedures, and incident response plans. By utilizing the HEAT methodology, an EMB assesses its current practice and anticipates possible weaknesses, unanticipated threats, illicit incursions, system failures, or unfounded legal challenges to help identify the areas in which an EMB needs to develop better strategies. The methodology then guides the EMB through reducing or eliminating different types of exposure in a systematic manner. K. Ellena et al. (2018, October 17). *Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies*. IFES. https://www.ifes.org/publications/cybersecurity-elections

integration into donor assistance programs, consideration should be given to the technological life cycle; technology must be updated, maintained, retired, and replaced. Introducing technologies also requires understanding security implications — even if the technology itself is being leveraged to solve a security problem. Donor organizations can assist EMBs to appropriately and transparently procure technology, train EMB personnel to utilize it, and provide other forms of advisory support and capacity development to help EMBs further utilize, access, and maintain relevant technology.

Once risks have been identified through an exploration of the context and threats in steps 1 – 4 above, solutions can be defined using the lens of people, processes, and technologies. For example, if there is a high risk of EMB staff clicking on malicious links sent to them in a fake invoice in an email which can install malware that compromises an EMB's network, then solutions can be defined using the following lens:

- **People**: Provide education and training components for users to help them recognize phishing links and take more appropriate action.

- **Process:** Develop an audit policy that evaluates employees and identifies users who click on malicious links more often than others so remedial action can be taken.

- **Technology:** Find and implement technological solutions that help prevent future compromise, such as virus scanning or technologies that strip links out of emails before users receive them.

These solutions are all examples aimed at the implementation level within an organization. Depending on the information gathered during the assessment and context surrounding a particular country, development programming may seek to influence an EMB toward such solutions, may directly support the implementation of such solutions, or may include components that help address the risk in some other way, such as by building capacity within the EMB to recognize and remediate risks internally.

The following section uses an important election process - voter registration - as an example to show the types of action that can be taken, and possible questions aimed at strengthening cybersecurity. Other election processes, such as those covered in the *Primer: Cybersecurity and Elections,* can be evaluated for risk and similarly addressed. Cybersecurity risks will be present whenever and wherever information technology is utilized across the election process.

Example: Addressing Voter Registration Cybersecurity Risk

When developing voter registration assistance programs, it is important to keep cyber security in mind. Voter registration creates a high risk of data and privacy breaches, because it includes distributed data collection activities and centralized data storage and processing. Whether a project has an explicit cybersecurity focus or a broader voter registration or election operations focus, it should include a component that addresses security concerns. Actions to strengthen the cyber protections for voter registration can be taken in technical assistance programs, including:

- *System architecture review*: Supporting outside experts to review system architecture (hardware, software, data communication) to identify vulnerabilities.

- *Analysis of data flows*: Collaborating with an EMB to analyze data flows, including input from other government agencies such as a civil registry, department of births and deaths, defense force deployment, ministries (internal affairs, justice, immigration), and points of data access by political parties, civil society, and voters. The analysis should identify points where data may be subject to unauthorized access, alteration, or disruption during intensive registration periods. This analysis can then help drive other possible assistance, whether through donor involvement or through implementing partners, offered to EMBs. This may include, for example, facilitating the drafting of formalized agreements between the EMB and various other departments to specify reciprocal security standards, roles, and responsibilities.

- *Security controls assessment*: Supporting the audit and assessment of existing security controls, such as security appliances and firewalls, assessing the implementation of regular firmware and software updates, antivirus software, and identifying and consulting on the training needs in cases where staff do not have the capacity to properly configure and maintain the control systems. The results of these assessments are the basis for further capacity building, such as supporting workforce training, helping EMBs procure professional support services from original equipment manufacturers, upgrading legacy and out-of-support hardware and software, and integrating IT good practice into EMB operations.

- *Incident response plan assessment*: Determining whether there is an incident response plan, either at the top EMB-level or within the Voter Registration or IT Department, and whether appropriate staff have a clear understanding of how to respond to a cyber incident. EMBs can be supported to build incident response plans through training, through contracted advisor or consultant services to fill important work roles that are not staffed, and through facilitation of constructive collaboration between EMBs and other agencies to define roles and responsibilities.

- *Procurement and supply chains policy review*: Reviewing procurement policies and processes and supply chains to detect potential vulnerabilities to attack during the production, shipping, and storage of systems. EMBs can be supported to identify reputable providers of products and services and instructed on good practice to follow for sensitive equipment and services procurement.

The above activities should be integrated into the broader project as appropriate. For example, if the project has a general election cybersecurity component, activities should be included to assess all critical information assets, including voter registration, party and candidate registration, ballot production and e-voting or election results management system, among other components. Or if the project has a specific voter registration component, it should include cyber assessment activities along with analysis of registration laws, identification documents, deterrence against duplicate or fraudulent registration, procurement of systems, and so forth.

Section IV: Electoral Cybersecurity Programming

For development assistance to be effective, it should be informed by and aligned with the steps detailed in section III, using the different assessments as a baseline to identify challenges, needs, and opportunities in the electoral process. To help determine the scope and size of the necessary programming, donors should establish realistic objectives, adopting the systems-based approach outlined above. The following section provides an overview of common approaches to cybersecurity programming, which can either be developed into stand-alone projects or incorporated into more traditional electoral assistance projects. Programming approaches highlighted include:

- Ensuring a well-defined regulatory framework
- Supporting a long-term EMB cybersecurity strategy to include:
  - Encouraging the formalization of an EMB audit process for election data
  - Assisting technology procurement and the creation of technology procurement practices
  - Advising on the responsible implementation of new technology
- Building confidence through a comprehensive communications strategy
- Supporting regional and global networks for electoral cybersecurity

A. Ensuring a Well-Defined Regulatory Framework

Cybersecurity assistance can focus on developing and updating the relevant legal and regulatory framework. At least 156 countries have enacted cybersecurity laws, including 91% of European countries and 72% of African countries. Even in the most advanced legal and regulatory frameworks, legislators face challenges due to the rapidly changing landscape and limited expertise.[24] There are at least three programming categories that may assist with the development of an effective regulatory framework to deter cyberattacks in elections.

- First, **direct assistance to EMBs**, and to judicial branches, the legislature, and oversight institutions involved in election oversight or dispute resolution can provide needed technical advice on cybersecurity strategies, organizational structures, and legal frameworks. Assistance can focus on the following goals:

  - Better define roles and communication mechanisms among organizations with responsibility for regulation and enforcement. This can be achieved through coordination meetings among the key stakeholders.
  - Provide comparative analysis on international legal frameworks related to cybersecurity to inform in-country discussion and identify key issues for legislation or regulations to address.
  - Organize drafting workshops to create draft legislation and/or procedures related to national cyber issues.

- Second, **efforts to promote a robust regulatory framework** can begin by commissioning an independent review of the legal framework for elections by international or domestic experts.

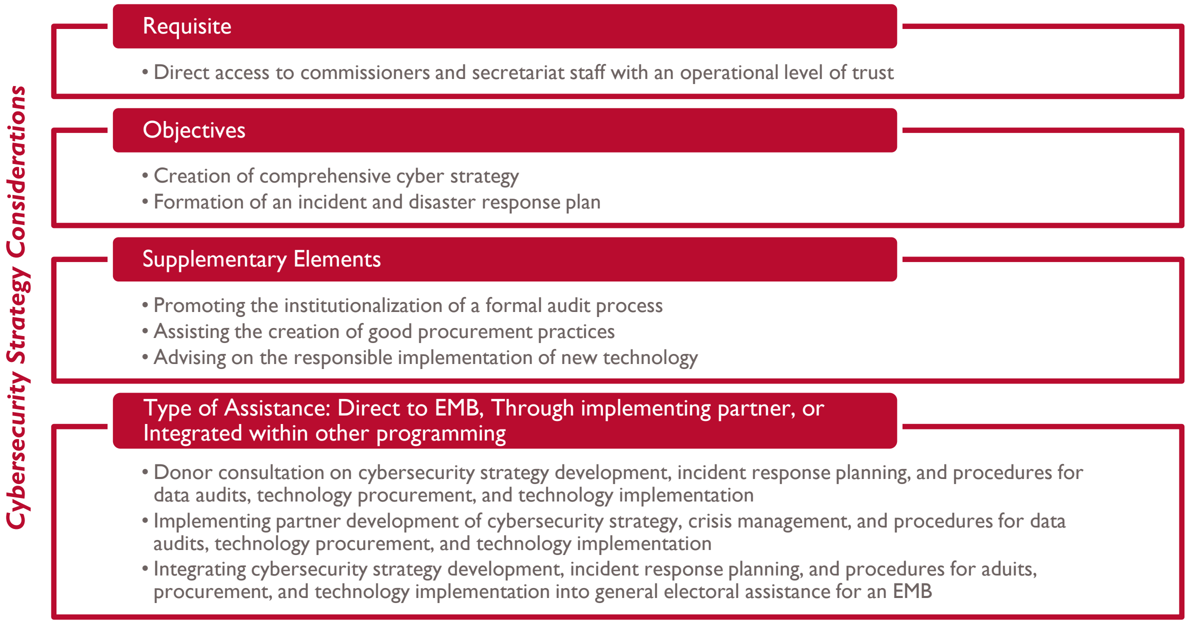
[24] United Nations Conference on Trade and Development (UNCTAD) (2021, December 14). Cybercrime Legislation Worldwide. https://unctad.org/page/cybercrime-legislation-worldwide

This could include recommendations for strengthening the laws protecting against cyber interference in elections and could build support among electoral stakeholders for reform. Ideally, to identify concrete steps toward national reforms, these recommendations would be followed by consultative meetings and coordination among government and private sector agencies involved in national cybersecurity.

- Third, international assistance can support the **development or strengthening regional bodies** to share information and coordinate the development of cybersecurity protections. A regional body may be formally established as a regulatory agency, such as the European Union Agency for Cybersecurity (ENISA), or it could be an election-specific regional association such as the Association of Asian Election Authorities (AAEA). Projects that work with an association of electoral authorities should help expand communication and exchange between EMBs related to cyber threats and help develop cybersecurity expertise and capacity within regional bodies.

B. Supporting a Long-Term EMB Cybersecurity Strategy

In cases where there is already significant trust between the EMB and USAID (or between the EMB and the implementing partner), it may be possible to support the EMB in creating or improving its cybersecurity strategy. Under-resourced EMBs may not have a formal cybersecurity strategy and rely instead on a patchwork of guidelines for staff to follow when it comes to cybersecurity practices and protocols. This often leads to ad-hoc and unsustainable solutions and an absence of well-understood standard operating procedures. It should be noted, mature cybersecurity programs are proactive in thinking through emerging and changing risks, often adapting to new context and threats.



Cybersecurity Strategy Considerations

Requisite

- Direct access to commissioners and secretariat staff with an operational level of trust

Objectives

- Creation of comprehensive cyber strategy
- Formation of an incident and disaster response plan

Supplementary Elements

- Promoting the institutionalization of a formal audit process
- Assisting the creation of good procurement practices
- Advising on the responsible implementation of new technology

Type of Assistance: Direct to EMB, Through implementing partner, or Integrated within other programming

- Donor consultation on cybersecurity strategy development, incident response planning, and procedures for data audits, technology procurement, and technology implementation
- Implementing partner development of cybersecurity strategy, crisis management, and procedures for data audits, technology procurement, and technology implementation
- Integrating cybersecurity strategy development, incident response planning, and procedures for adults, procurement, and technology implementation into general electoral assistance for an EMB

A program assisting the creation of a cybersecurity plan should already have access to commissioners and secretariat staff who will be involved in drafting, reviewing, and implementing the plan and who trust the implementers. To create a cybersecurity plan, the program should:

- *Conduct an EMB security landscape assessment*: Assess the EMB's current security landscape (which may already have been done if the four-step process outlined earlier is being followed), including risk analysis. Ideally, this program would also assess relationships with other states and possibly private institutions assigned responsibility for national cybersecurity. In cases where there is not an existing link between the EMB and these organizations, it may be helpful to facilitate a joint training session around cybersecurity and elections. The output of the mission is a comprehensive document that includes a risk analysis, the current inter-relationships of institutions, and recommendations for next steps to improve preparedness to thwart or mitigate any cyber attacks.

- *Develop a comprehensive security strategy*: Develop a comprehensive security strategy that addresses all potential threats that were identified during the risk analysis. The security strategy will require problem solving and expert recommendations for accommodating resource and personnel limitations as well as the appropriate emphasis on areas where effective and efficient improvements can be made. Again, this should include other organizations charged with national cybersecurity, as well as commissioners and senior staff from the EMB. If there is preexisting coordination between institutions involved, the security strategy can be an output of the cybersecurity assessment mission described in the previous bullet point. Alternatively, it could be a follow-up mission if there is a need to disseminate the assessment report and build consensus among institutions that a joint effort is appropriate.

- *Create incident response and disaster recovery plans*: Create incident response and disaster recovery plans to improve response time in case of an attack or other security breach. This plan can be informed by tabletop exercises or scenario simulations where EMBs identify the areas in which response procedures are lacking or exposure is the most dangerous. A plan may be broad in nature, developed as an output of the previously described exercise(s), or specific, developed as part of existing support to an activity such as voter registration or election results management. In either case, it should be developed by the EMB with guidance from experts. EMB staff are more qualified to create a realistic plan according to time limitations and resources in the face of other demands during each phase of the election cycle. The implementing partner can facilitate the drafting of a plan by providing guidance during a workshop that helps the EMB set aside adequate time to draft a plan.

- *Plan and begin necessary integrations to manage strategic communications*: Incorporate crisis communications strategy and protocols into the incident response and disaster recovery plans to inform an EMB's public relations approach in the event of an incident, attack, or security breach. The importance of perception and narrative control should not be minimized; a crisis communications strategy can be a strong second line of defense for an EMB in a crisis. Although a general elections communication strategy (see below on *Building Confidence through a Comprehensive Communication Strategy*) can provide helpful context, crisis communication should include specific plans related to information exchange, chain of command for decision-making, how much detail to share, and whether there are legal requirements to disclose certain information in case of a breach, and how to address concerns raised by political actors and the media. The development partner can help create a crisis communication plan through training and tabletop exercises that provide adequate time to develop and refine the plan. Development of a crisis communications plan is not a trivial process;[25] Expert leadership can be crucial to guiding the EMB and partner organizations in defining effective strategies and templates for communicating efficiently while also managing other aspects of crisis management. The plan should identify weaknesses in the EMB's ability to implement the security strategy and include recommendations for how to address these weaknesses. The recommendations may include upgrades to the cyber security infrastructure or additional technical training to address any deficiencies in staff capacity.

- *Support staff cybersecurity and electoral operations training*: Prioritize staff training on cyber hygiene as well as general electoral processes related to their particular responsibilities. The plan should include a strategy for training staff as well as regular reminders to increase awareness of the security plan and general cyber hygiene practices. Cyber hygiene training is a flexible program activity that can be provided as part of a standalone cybersecurity project or as an integrated cybersecurity component within specific electoral activities, or as a standalone activity. This training is also a good "ice breaker" activity that can help build trust with an EMB that is not open to other types of assistance.[26] Cyber hygiene training is not only critical for the success of cybersecurity efforts but can be an entry point to engage with EMBs who may be hesitant. According to IBM's Cyber Security Intelligence Index, 95 percent of all security incidents involve human error.[27] Cyber hygiene training is designed to reduce risk of human error, meaning it provides strong protections to the EMB, and has the advantage of being a non-controversial offering EMBs are likely more open to.

- *Update and review schedules:* Incorporate periodic updates and reviews of security plans and cybersecurity strategies. Because electoral processes and threats to those processes are continuously evolving, the security plan should include a schedule for regular review and updating. Periodic reviews are best incorporated into longer projects where the development partner will be around to help guide the review. In shorter projects the review can be added to the calendar and emphasized as a critical activity.

B.1 Encouraging the Formalization of an EMB Audit Process for Election Data

The principles of secrecy of the vote and personal data privacy place restrictions on the transparency of certain types of election data that make audit practices essential. Programming approaches should

[25] Although related to public health rather than elections, the Centers for Disease Control (CDC) has a Crisis and Emergency Risk Communication (CERC) manual that demonstrates the amount of work and steps that go into creating a crisis communication plan. *See, CERC: Crisis Communication Plans* in CDC (2014). *Crisis and Emergency Risk Communication.* U.S. Department of Health and Human Services. https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf

[26] For example, IFES' cyber hygiene curriculum was one of the earliest components of IFES's program in Ukraine and provided an entry point that rapidly expanded to creation of the "IFES Ukraine Cybersecurity in Elections Playbook," *see* Petrov, G. and Chanussot, T. (2018, November). *A Cybersecurity Playbook: Combating Threats to Ukrainian Elections through Good Practice.* IFES. https://ifesukraine.org/wp-content/uploads/2019/02/IFES-Ukraine-Cybersecurity-in-Elections-Playbook-v1-2019-02-15-Eng.pdf. The cyber hygiene training covered a wide range of topics including phishing and spear phishing, password best practices, data backup and protection, software updates and antiviruses, clear desk and clear screen policy, USB device hygiene, dangers of the Internet of Things (IoT), and Social Networking.

[27] Security Intelligence (2015, June 3). *2016 IBM Cyber Security Intelligence Index*. Advanced Threats. https://securityintelligence.com/media/cyber-security-intelligence-index-2015/?mhsrc=ibmsearch_a&mhq=cyber%20security%20intelligence%20index&_ga=2.18516401.982110719.1676526760-1291583095.1676526760

utilize both internal and external, independent audits, while also building capacity for the EMB to support periodic audits in the future.

Audits of EMB practices can be conducted internally by the EMB or by an external impartial organization. Internal audits help detect errors in the system or manipulation by hackers; external audits are more effective at increasing public confidence. Ideally, the EMB conducts regular internal audits and invites external audits after each major exercise or as needed if there is a lag in confidence or if allegations or errors are raised by political parties or candidates.

The donor should plan for building long-term EMB capacity to conduct audits on its own when encouraging or promoting the formalization of audit processes of EMB data. In the program design, development assistance can focus on creating processes for internal or external audits, whether conducted by an external partner or by the donor or implementing partners as a part of EMB capacity-building efforts. Whether supported by the donor or implemented by partners, internal and external audits should include several specific elements.

EMBs conduct internal audits to detect potential problems and identify ways to improve the process. These audits usually consist of:

- Analysis of data logs and anomalies in data entry – such as mass injections of data from a single systems user in unrealistically short periods.

- Data integrity tests that can detect anomalies in demographic distribution, date/time of registration, and geographic encoding errors, among other factors.

Donors can help the EMB to institutionalize internal audits by supporting training and expert assistance with early audits to demonstrate the value they can provide.

External audits are often conducted by domestic civil society organizations, with donors providing both funding and expertise to guide the exercise. While internal audits help the EMB to improve, external audits are aimed at improving public confidence. The external audits may add:

- Reviews of the legal and procedural framework for registration and training materials to determine whether there are barriers that may prevent or encourage registration.

- Investigation into any specific allegations of voter data manipulation.

- Field exercises, including list-to-voter and voter-to-list surveys to independently assess whether voters lists are accurate, complete, and up to date.

- Analysis of security measures in place to protect against unauthorized access to voter data.

- Audits of election results are most useful when there is a source of data to compare against the official count. Such external sources may include a voter-verifiable paper audit trail (VVPAT), copies of results forms posted in polling stations, tabulation logs at regional or central offices, correction forms completed if a supervisor corrects data reported by a polling station, and, when available, parallel vote tabulation data.

Example: Kenya

In Kenya's 2013 election IFES assisted with an internal audit of the results transmission system that included live monitoring of all network activity on the closed results transmission network. Only one intrusion was detected when a journalist unplugged a network cable from one of the computers provided for media and tried to connect to his laptop. The internal audit reports, however, did little to allay the opposition's suspicions that were fueled by the losing candidate's claims that he had been cheated by a hacker who altered the results. Assisted by NDI, a consortium of CSOs, the Election Observation Group (ELOG), conducted an external audit, consisting of a parallel vote tabulation (PVT) that validated the results published by the EMB. The ELOG report was key to defusing a volatile post-election environment.

Election results data differs from other government and business data because it must maintain the secrecy of the vote. This can be illustrated by the common, yet erroneous, comparison between voting systems and banking systems, reflected in the question, "If I can trust an ATM or the internet with my money, why can't I trust an electronic voting machine or the internet for voting?" The reality is that no one needs to "trust" an ATM or internet banking system; every account holder can track deposits and withdrawals and can thereby verify the accuracy of every electronic banking transaction. Vote counting systems have different requirements related to the secrecy of the vote. By design, no one can know the specifics of every ballot counted by the system. If an attacker can gain access to the vote counting program and change it to skew the vote, the modification would be difficult to detect without an external audit mechanism. For this reason, international best practice is for voting machines to include a VVPAT. The VVPAT can be used for a manual count to verify that the machine accurately recorded the votes cast. Manual audits of the vote count – which, for example, can compare each voting machine's VVPAT results with the electronic results – are an established good practice that can be done in various ways, from 100% manual verification to random manual audits (RMA) to risk-limiting audits (RLA).[28]

There is a similar issue with voter registration data. Because of data privacy regulations in some countries, political stakeholders cannot track every new registration, modification of voter data, or deletion of voters. Even where there are no data privacy regulations, the sheer volume of data makes it difficult to track every change. If an attacker is able to gain access to the voter registration data, it is quite possible that they could make modifications that would influence the outcome of an election without detection. A voter register audit provides an in-depth analysis of the voter registration data to detect anomalies in demographic distributions, geographic encoding, and other data to verify the integrity of the voter register.[29] Such an audit can be done as a one-time exercise or it can be a part of the regular data processing procedures.

[28] For an application of RLA to the global electoral context, *see* Shein, E. and Brown, A. (2021, March 2). *Risk-Limiting Audits: A Guide for Global Use.* IFES. https://www.ifes.org/publications/risk-limiting-audits-guide-global-use

[29] In 1999, one of the earliest audits of a voter register in Guyana detected an anomaly in the database design. The encoding of electoral districts assigned values of 01, 02, etc. to the ten districts. More than 5,000 voters were missing from the register in an opposition stronghold. The audit revealed that the missing voters had been entered as residing in district 1 rather than district 01 and were consequently omitted from the provisional voter lists. Although the

B.2 Assisting the Creation of Technology Procurement Practices

Donors who provide procurement assistance for any new technology should ensure that the EMB establishes a process for developing specifications. Helping EMBs develop sound procurement policies can help address critical weaknesses by including vetting of vendors and components and ensuring that procurement committee members are impartial. Even if the donor is not contributing to the cost of the new equipment, EMBs can benefit from technical assistance on how to shield against vulnerabilities that may be introduced by the procurement process. Donors may support training or orientation on procurement laws and procedures, though any training should be coordinated with the EMB to avoid duplication. Programming may go beyond fundamental legal requirements to address ethical considerations for members on procurement committees, and the negative consequences that any procurement irregularities may have on elections. Training should underscore the responsibility to report any improper communication from any vendor or vendor representative, particularly on how to respond in cases of threats or offers of bribery.

Technical assistance can help ensure that the EMB creates policies that address how the procured system will be used, who should have access, how data will be stored and shared, and whether there are appropriate policies to protect against improper use of any personally identifiable information. The procurement plan for any new technology should include parameters for the anticipated life cycle of the technology, contract provisions to ensure that replacement components will be available throughout the lifecycle, and policies to ensure that no new vulnerabilities are introduced by the replacement of components or malfunctioning systems.

Although the donor may have a much greater say in the procurement and deployment process if its funds are used, any project in which a donor has an active role in providing technical advice to an EMB should offer assistance in protecting against cyber threats that may be introduced by new technology. That starts with the creation and retention of good procurement practices.

B.3 Advising on the Responsible Implementation of New Technology

In addition to advising on or co-creating EMBs' technology procurement policies, EMBs, donors, and implementing partners should also pay special attention to how new technology is selected and deployed. The risks created by implementing new technology range from poor configuration, lack of technical knowledge, inadequate timeframes for deploying and testing, and proper backups for technical failures. The overall cybersecurity strategy of the EMB should include steps for reducing risk when selecting and deploying new technologies. Therefore, standards or requirements for technology implementation should be built into program design. Development projects could begin with an entry point either providing direct cybersecurity assistance or aiding with introducing the new technology such as voter registration kits, vote counting technology, electronic voting machines, or other election technology. Whether it is helping to draft overall cybersecurity strategies or deploying new technologies, activities could include some or all of the following:

audit was not able to determine whether the miscoding was accidental or deliberate, or even whether it may have been altered by someone who gained unauthorized access to the database, it did allow for correction of the problem without conducting a new voter registration as the opposition party was demanding. This audit was conducted by the author and another expert.

- Security assessments and penetration testing during the development or configuration of the new technology, before accepting delivery.

- Ensuring that all commercial-off-the-shelf (COTS) technology, both hardware and software, is updated with all recommended security patches.

- Defining and reviewing steps for configuration of systems after delivery.

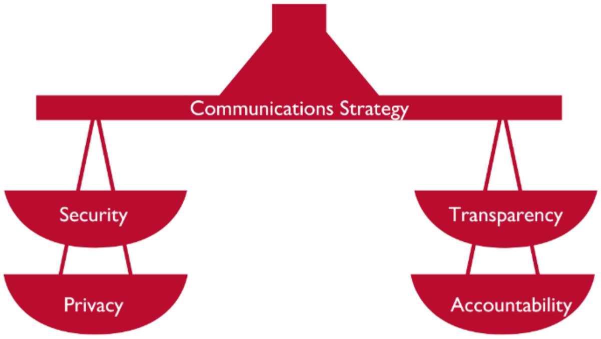
- Assessing training requirements for staff who will use the new equipment, with a focus on cyber hygiene best practices.

- Analyzing data flows into and out of the new system and how existing networks will be impacted, whether proper network segmentation rules are enforced, and whether existing security appliances are adequate to monitor for any new threats or suspicious activity related to the new technology.

- Defining an incident response plan so all staff will know how to respond in case of a security breach or cyber attack.

- Ensuring that procedures are in place for backup of all data captured or generated by the new system.

C. Building Confidence through a Comprehensive Communication Strategy



Electoral processes and – more specifically – EMBs face immense public scrutiny, and building voter confidence in the process is very challenging in most contexts. Malign actors may attempt to manipulate elections directly, undermine public confidence in elections, or erode the legitimacy of elected representatives and bodies by exploiting vulnerabilities in electronic information processing and cyberspace. Such weakening of trust and legitimacy could impede development initiatives and undermine effective and accountable governance.

Public confidence is an essential consideration when developing EMB policies, procedures, and cybersecurity. To earn public confidence, accountable, inclusive, transparent, and *secure* electoral processes are fundamental. As part of this, transparent communication practices can go a long way to foster public confidence in an EMB. Consequently, development assistance should consider programming that helps EMBs with strategic and crisis communications to facilitate public confidence in elections. Donors can provide guidance to EMBs or instructions for implementing partners to help build a proactive and comprehensive communication strategy that not only is prepared to address crises but also to promote dialogue between key stakeholders. Although some EMBs may be reluctant to expand communications with stakeholders who are too adversarial, experience in many countries has demonstrated the value of efforts to build rapport.

Voter confidence can be shaken or undermined if election processes aren't transparent and easily understood. If a process is hard to understand, election dispute resolution can become difficult and voter confidence can be further affected. Therefore, when, for example, an EMB deploys new technologies in its election process, it is not enough to merely protect against attacks. Presumably, technology was introduced to address specific problems or provide significant improvements to the electoral process. Proper attention must be paid to educating stakeholders, including voters and political parties, in the value or necessity of this technology.

Consequently, development assistance should help an EMB build a communication strategy that properly informs political stakeholders and the public about the technology used in the election process, from its benefits to how data is protected and votes are tabulated. A broad communication strategy should address voters, political parties, and other key stakeholders, including poll workers and judges.

A communication strategy that encompasses all stages of the electoral process helps the EMB to progressively build public confidence in the process as well as respond to crises as they emerge. Returning to the example of introducing new technology, well-developed voter education and awareness campaigns help build foundations of transparency and general understanding of the electoral process. These campaigns could communicate how a new system will help ensure more efficient, secure, and accurate updates to the voter register or other elements of the election process a new technology may aid. Communication plans should also address concerns about potential cyber threats related to the election process, especially when introducing new technology, as well as assurances about the steps that have been taken to protect against such threats.

Donor assistance for communications strategy development can include:

- Technical assistance on strategic and crisis communication planning to inform the public of election technology and efforts the EMB is taking to secure against cyber threats.
- Capacity building, including one-on-one communications consultations with EMB officials, to help build comprehensive communication practices.
- Integrating crisis and strategic communications surrounding election technology and cyber threats into wider donor assistance to confidence building in the election process. This includes advising on or prescribing general communications strategy development with a variety of election stakeholders, such as EMBs, political parties, and other relevant institutions.

By assisting an EMB in creating and executing a comprehensive communication strategy, an EMB is well-positioned to build public confidence in the electoral process. Additionally, a communication strategy helps an EMB demonstrate its independence and impartiality, which further contributes to voter trust and confidence in the institution itself.

D. Supporting Regional and Global Networks for Electoral Cybersecurity

Many cyber attacks on the election process are launched by actors outside the country or region in question. This complicates the task for individual EMBs to protect their networks and processes and makes it difficult or impossible for national authorities to investigate and prosecute many cyber attacks. While there are considerable variations in the contexts in which EMBs may operate, there are still common threads when it comes to their electoral cybersecurity. Thus, national, regional, and global networks[30] for standardization, best practices, and lessons learned on cybersecurity can serve to orient any EMB in its efforts to identify threats and build comprehensive responses to those threats.

These networks can facilitate knowledge sharing and lessons learned, especially as new technology, software or hardware, and cyber threats emerge in the election space. Through networks, EMB representatives can convene around a particular aspect of the electoral process, such as voter registration or results management systems, to draw on input and experiences from other regional EMBs or internationally accepted practices. Alternatively, these networks can provide EMBs with a place for information sharing and threat analysis to create shared responses and best practices to combat common threats to election security as a whole.

Regional associations of election officials have been operating since the 1990s, though the past few years have been difficult for most.[31] Nevertheless, there are a growing number of regional cybersecurity networks, such as the Cybersecurity Network of the Americas (LATAM CISO) and the European Union Agency for Cybersecurity (ENISA). It is not yet clear what the most effective approach to creating effective regional networks for sharing information about election cyber threats is; however, possible approaches include introducing cybersecurity programming to a regional association of election officials, helping to create a focus on election security in the regional cybersecurity networks, or a hybrid of the two.

EMB strengthening activities could help the EMB establish communication with both regional election associations and regional cybersecurity associations to explore levels of interest and capacity to incorporate information sharing mechanisms and for collaboration on incident response. To build trust between both types of organizations, an initial activity that invites members to a joint training and planning workshop to increase understanding of the evolving threat landscape facing election administrations, with discussion of possible mechanisms for sharing, could be beneficial.

Section V: Conclusions and Recommendations

Cybersecurity must be treated as an issue that has moved from the periphery to center stage for EMBs and their partners in election management. It will continue to gain importance as election processes continue to be digitized and, in some cases, brought online. As the scale and sophistication of cybersecurity threats continue to grow, EMBs will need significant support developing their internal cybersecurity

[30] An example of a global network is the Global Electoral Organization (GEO) Conference. The GEO Conference has been held seven times since its inception in 1999, with the last conference in 2016, hosted in Washington, DC by IFES. The conference brings together election professionals from all over the world to share experiences, achievements and lessons learned. Past conferences have been sponsored by IFES, International IDEA, Association of European Election Officials (ACEEEO), Electoral Institute of Southern Africa (EISA), Carter Center, Elections Canada and UNDP, with additional funding from donors and exhibitors showcasing election commodities and technologies. Plans for a 2020 conference were thwarted by the COVID pandemic, but may be revived in the future. IFES (2016, November 6-10). The Seventh Global Elections Organization Conference (GEO-7). https://www.ifes.org/events/seventh-global-elections-organization-conference-geo-7

[31] The Association of European Election Officials (ACEEEO) was dissolved in March 2022 over a failure to reach agreement over whether to expel the Russian and Belarusian EMBs in response to the invasion of Ukraine. However, Association of African Election Authorities (AAEA), Association of Asian Election Authorities, and Latin American Council of Electoral Experts (CEELA) are all still functioning, though activities seem to have been curtailed since the advent of COVID.

capacity and establishing much-needed cybersecurity risk management programs. In many places this capacity building will require not only financial investment but strategic and operational support and advice. In addition to programmatic support, USAID and the broader development community will play a crucial role as trusted advisors and interlocutors.

Any plan to introduce electoral cybersecurity programming should begin with an assessment of the electoral environment, including potential threats, EMB partnerships with other institutions engaged in national cybersecurity, the cybersecurity capacity of the EMB, and the level of openness to donor assistance. Tools such as USAID's Digital Ecosystem Country Assessment (DECA) can provide context assessments, while framework tools such as USAID's Electoral Assessment Framework can help to identify challenges, determine priorities, and establish objectives for electoral assistance programming. Reports by election observers and implementers provide valuable historical context related to any progress or setbacks by the EMB in addressing key challenges and concerns voiced by political stakeholders. The assessment should include interviews with key commissioners and staff, representatives of political parties and civil society organizations, and where feasible, officials of government agencies responsible for national cybersecurity. These interviews serve to gather additional information, gauge openness to assistance, and help to build preliminary buy-in for proposed assistance.

The type of programming appropriate for the environment must take into account the level of trust from the EMB, and whether donor assistance is perceived as helpful or a threat. EMBs may feel threatened by the possibility of interference, the exposure of their weaknesses, or concerns about political responses to the type of assistance offered. The resiliency of a country in the face of cybersecurity threats is multi-faceted and consists of not only EMB cybersecurity capacity, but also the cybersecurity capacities of stakeholders that engage across the electoral cycle. The following types of activities can help EMBs and stakeholders build, sustain, and grow their cybersecurity capacity:

- **Support efforts to promote robust regulatory frameworks.** Donors can support EMBs and other involved stakeholders to understand the importance of robust, clearly defined, and well-supported regulatory and policy frameworks. This may include helping judicial and executive branches of government better integrate election technology considerations into their existing regulatory and policy contexts, clarifying how election dispute resolution involving technology, election technology procurement, and security standards are reflected within national policy and legal mechanisms.

- **Promote and support training and technical assistance to build cybersecurity capacity among EMB staff and other stakeholders, including technical staff training, general elections staff and volunteer training, and executive-level training.** At each stage of the election process, there are multiple constituencies, including government officials, EMB staff members, and others responsible for implementation of specific election tasks. Through assessment, training, technical assistance, and capacity building for both general cybersecurity practices and secure electoral processes, the involved parties will be better equipped to adopt and implement proper cybersecurity procedures throughout each part of a complex endeavor. For example, training for designated IT and cybersecurity personnel to secure networks, respond to incidents, test security controls, and auditing policies, processes, and programs. The introduction of a basic cyber hygiene training focused on individuals with access to sensitive data, such as staff within an EMB or to educate volunteers at polling locations, can help prevent techniques such as phishing, as users are prepared to recognize and mitigate them. Finally, exposing executive leadership to cybersecurity management skills can arm them with knowledge to support establishing and sustaining robust cybersecurity risk management programs and policies. With sound understanding of cybersecurity threats and approaches, EMB executives can be empowered to make resource decisions that integrate security holistically across the election process.

- **Support EMBs in strategic planning that integrates a life-cycle approach and cybersecurity 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 cybersecurity 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 beginning during planning phases.

- **Assist EMBs in cost-effective and transparent procurement practices and, when appropriate, help procure secure technology and infrastructure.** Election infrastructure often lacks current generation security due to resource constraints, lapses in robust IT life-cycle practices, and procurement and deployment timelines that do not line up with commercial technology cycles. Donors can help bridge this gap through targeted procurement assistance, consultation, and advisement on technology options. This may include helping procure technologies like firewalls and security specific hardware and software; it can also include helping EMBs make use of secure cloud services to store and process election data. To the extent that third-party service providers are utilized, EMBs can be 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.

- **Support EMBs to build robust internal audit capabilities and support external audits of EMB cybersecurity policies, procedures, and practice.** Audits of EMB practices can be conducted internally by the EMB or conducted by external impartial organizations. Internal audits can help detect and prevent cybersecurity breaches while also helping ensure robust cybersecurity implementation. External audits are also useful for the same reasons and effective at increasing public confidence as well.

- **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, particularly when an incident response is ongoing. Independent of any incident, EMBs can help build in 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.

- **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 election 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 can facilitate knowledge-sharing and learning, especially as new technology, software, and cyber threats emerge in the election space. This may also include a focus on cybersecurity at already established elections focused communities and networks to better integrate cybersecurity into the election focused development assistance ecosystem.

Where possible, assistance should build toward development of an integrated cybersecurity strategy for the country. Stakeholder and public confidence can be fragile, and it is far easier for a detractor to damage this confidence by allegations of a cyber attack than to mount a successful cyber attack. All improvements to security should, to the extent possible, help to improve stakeholder and public confidence that the EMB is effectively identifying and addressing potential threats.

In cybersecurity, as in many development activities, consistency trumps intensity. The growth of cyber threats has far outpaced EMB cybersecurity development. While every project that strengthens election cybersecurity is important, and while intense activities may provide immediate protection to a network or an electoral activity, a lack of consistency will result in rapid erosion of that protection. Consistency, on the other hand, ensures that security measures are continuously monitored and updated to reflect changes in technology, threats, and vulnerabilities. Consistent programming is also needed to build a culture where cybersecurity is viewed as a top priority, and where everyone is responsible for maintaining the security of the electoral systems and processes. Cyber threats to credible elections have grown rapidly over the past decade, while EMBs, governments, and development assistance programs have been slower, but building momentum. Cybersecurity assistance programming has demonstrated that donors can play an important role in raising awareness about threats, developing cooperation between EMBs and national security agencies, and building effective cybersecurity infrastructures.

Creating an effective cybersecurity environment is not a one-off exercise; cybersecurity should be considered as an integral part of all plans to provide development assistance to elections. While one-off interventions may be necessary at times to address specific threats or to protect specific electoral exercises, long-term consistency is key to building and maintaining effective election cybersecurity programs.