USAID
FROM THE AMERICAN PEOPLE

AN ELECTRONIC BALLOT BOX USED IN REMOTE LOCATIONS IN BRAZIL, COURTESY OF IFES

Primer: Cybersecurity and Elections

JULY 2022

USAID
FROM THE AMERICAN PEOPLE

DAI
Shaping a more livable world.

International Foundation
for Electoral Systems

Acknowledgements

This primer 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). Dr. Tarun Chaudhary was the lead author. The primer benefited tremendously from contributions by Matt Bailey, Dr. Staffan Darnolf, Chelsea Dreher, Erica Shein, and Annie Styles. The team is grateful to those individuals who reviewed various drafts and provided valuable insights.

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

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

CONTENTS

Section I: Introduction

The goal of this primer is to support United States Agency for International Development (USAID) Democracy, Human Rights, and Governance (DRG) personnel, as well as the broader DRG community, to understand the challenges posed by cybersecurity in elections and better integrate cybersecurity assessment and readiness into relevant electoral and political processes programs. This primer:

- Identifies potential impacts of cyber attacks on electoral and political processes;
- Introduces basic principles of cybersecurity;
- Characterizes risks in key components of the electoral process;
- Describes cyber threat actors, their motivations, and common tactics and attacks they may use; and
- Introduces industry-standard frameworks that can help guide election management body cybersecurity planning and strategy.

Planning and administering democratic elections is one of the most complex endeavors a country may undertake. The institutional context for election management can vary, but the core organization charged with administering a country's election process is commonly referred to as an election management body (EMB). The EMB typically has multiple responsibilities, including maintaining integrity throughout planning and preparation processes, carrying out election operations, and finalizing results. Information technology is being increasingly integrated into the planning, management, and execution of elections. As such, an EMB's mandate to protect the integrity of an election naturally extends to ensuring adequate cybersecurity for the information technology infrastructure used in activities under its purview. The term "cybersecurity" refers to how electronically processed information can be secured against disruption, disablement, destruction or malicious control, thus protecting its confidentiality, integrity, availability.[1]

Cyber attacks against public institutions – including those associated with election infrastructure – are occurring with increasing frequency globally.[2] Malign actors, whether foreign or domestic, use technology

[1] Please see the U.S. National Institute of Standards and Technology's (NIST) Glossary for definitions. National Institute for Standards and Technology. (n.d.). Glossary. https://csrc.nist.gov/glossary/term/cybersecurity.

[2] 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 experienced a hack of their Electoral Commission 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.

to enhance their reach and the damage they can inflict. Even as cyber attacks become more frequent, electoral processes are becoming increasingly reliant on the kinds of technology those attacks exploit. Elections increasingly depend on technology such as digital voter rolls and election results, biometric voter registration, and electronic voting machines.[3] The public is generally aware that these attacks are likely, and many doubt – often with good reason – that their countries are prepared to successfully counter them.[4] As technology changes, EMBs and their partners must adapt how they conceive of security to address and anticipate evolving threats.

Section II: Understanding Electoral Cybersecurity as a Development Challenge

While the world has generally moved toward use of election technology to digitize voter registers and transmit and aggregate election results, some countries have stepped back from digitizing the voting process due to security and transparency concerns.

For example, biometric voter verification machines have been introduced in Kenya[5] and Ghana,[6] biometric voter registration in Zimbabwe,[7] and electronic results transmission in Nigeria.[8] At the same time, countries such as Norway[9] and Germany have piloted electronic processes and subsequently decided against pursuing them further, due to lack of trust across stakeholders that include political parties, voters, and election managers or due to legal uncertainties and challenges.[10]

---

https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democratic-elections-latin-america; US elections have been targeted with cyber attacks, as have the 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.

[3] K. Ellena et al. (2018). Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. IFES.

[4] 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 Publics Brace for Cyberattacks on Elections, Infrastructure, National Security. Pew Research Center.

[5] Independent Electoral and Boundaries Commission (n.d.). Biometric Voter Registration System (BVR). https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR)

[6] Daily Mail GH. (2020, November 7). *74,800 new biometric verification devices procured for Dec 7 polls – EC.* https://www.dailymailgh.com/74800-new-biometric-verification-devices-procured-for-dec-7-polls-ec/.

[7] For further insight into the Zimbabwean experience see IFES. (2019). *Biometric Voter Registration in Zimbabwe*. https://www.ifes.org/sites/default/files/biometric_voter_registration_in_zimbabwe_one_pager_september_2019_0.pdf.

[8] VOA (2022, February 25). *Nigeria's Vuhari Approves Election Law to Improve Transparency.* https://www.voanews.com/a/nigeria-s-buhari-approves-election-law-to-improve-transparency-/6459308.html.

[9] Seltzer, Larry (2014, June 30). *Norway internet voting experiment fails*. ZDNet. https://www.zdnet.com/article/norway-internet-voting-experiment-fails/.

[10] The German case is interesting in that a 2009 judgement deemed the 2005 use of the machines as unconstitutional based on questions of transparency. Though the judgement did not preclude future usage,

Failure to address cybersecurity risks inherent to the use of technologies across the electoral process can pose a critical threat to electoral integrity. Electronic information systems used across electoral processes are important components of critical national infrastructure that can be vulnerable to attack, regardless of whether they are stand-alone or connected through the Internet. As the number of election technology applications grows, the vulnerabilities to cyber attacks also grow.

The Internet, despite all the societal benefit and economic value it has helped create, has also created an arena of strategic competition and criminal activity. Elections have begun to attract the attention of a wider spectrum of threat actors. Threat actors may have a range of motives, from mischief to malice to manipulation. Actors seeking to manipulate the results of an election may have purely political or financial objectives, while others may not have an interest in seeing a particular candidate or party prevail, but rather seek to undermine the credibility of the electoral process or erode trust in democracy. There are well-known examples of cyber attacks that have focused on elections launched by well-resourced foreign state actors with the aim of undermining trust in democratic processes and the legitimacy of their outcomes.[11]

Elections can also be threatened by cyber attacks led by domestic actors. These actors may be politically, financially, or ideologically motivated, or seek to exacerbate domestic tensions for a variety of reasons and may operate individually or collectively. Like their foreign counterparts, they often seek to create tensions and sow mistrust in elections and democratic institutions. The emergence and increasing prevalence of these domestic actors in many contexts means that institutions charged with upholding the integrity of elections must also work to recognize and mitigate potential insider threats. Cybercrime as a Service (CaaS), in which criminals offer paying customers malicious services and tools, has emerged as a global market for the sale of increasingly sophisticated capabilities, further complicating the cybersecurity context for election managers and increasing the scope and severity of attacks by a widening spectrum of adversaries.[12] In short: the costs of conducting cyber attacks against elections are falling, placing these tools in the hands of a growing array of international and domestic actors.

German movement towards electronic voting did halt. See the full judgement at: Bundesverfassungsgericht. (2009). *Judgement of 3 March 2009.* https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html.

[11] For a useful summary of Russian activity see: Tennis, Maggie. (2020, July 20). *Russia Ramps up Global Elections Interference: Lessons for the United Sates*. 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, 11 September). *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.

[12] Hyslip, T. S. (2020). Cybercrime-as-a-Service Operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 815-846.

Election cybersecurity is an important element of democratic resilience. The electoral process is a central mechanism for connecting public interests and preferences to responsive governance, but only if it is secure, credible, and transparent. Cybersecurity – and the ability of election authorities to prevent and mitigate attacks on critical election processes – is an underpinning element of this process.

Unfortunately, even the *perception* of vulnerability of elections systems and institutions to being hacked can undermine citizen confidence and ultimately degrade electoral processes. The appearance of vulnerabilities combined with perceived inaction on the part of an EMB, for example, can serve to undermine public confidence in the EMB's ability to manage an election. Therefore, even if an EMB's cybersecurity is mature and effective, assuring the public of that fact is often just as important.

Anti-democratic forces, criminal elements, and other threat actors clearly view connected electoral infrastructure as an attractive target for mischief, malice, and manipulation. Attacks on this infrastructure can impede development initiatives, destabilize fragile institutions or peace processes, and undermine effective and accountable governance. By undermining public trust in the election process, the institution of democracy itself can be called into question by political forces wishing to institute more autocratic processes or otherwise undermine institutions.

Cybersecurity breaches can create significant consequences, including legal liability, for both the institution and individuals involved. For example: in the Philippines, in March 2016, the website of the Philippines Commission on Elections (COMELEC) was hacked and defaced by a group called Anonymous Philippines. The hacker group, LulzSec Pilipinas, also released extensive voter information, including fingerprints. Following the attack, the National Privacy Commission recommended criminal charges against COMELEC Chairperson Andres Bautista for negligence, stating that, "The lack of a clear data governance policy, particularly in collecting and further processing of personal data, unnecessarily exposed personal and sensitive information of millions of Filipinos to unlawful access." While the commission did not find Bautista guilty of helping the attack, it ordered COMELEC to implement new security measures. Less than a month later, after a computer containing biometric records of registered voters was stolen from a regional election office,[13] Chairperson Bautista was impeached and resigned. These types of attacks can potentially have lasting impacts on not only specific institutions and election managers, but also on the electorate's trust in voting processes and institutions and stakeholders that are involved with those processes.

EMBs and other stakeholders – from civil registry offices that are engaged in the voter registration process to law enforcement agencies that support election security – must make difficult decisions about where to direct limited resources. Even in well-funded commercial organizations, cybersecurity can easily be overlooked due to a mixture of complacency, lack of awareness and know-how, and discomfort with what

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

is seen as an opaque and technical field for specialists. Among EMBs facing competing demands and limited resources, cybersecurity often fails to get the attention it needs. It is therefore necessary to better and more consistently integrate cybersecurity into programs aimed at supporting and building capacity of EMBs and other key electoral stakeholders.

Section III: Core Concepts of Information Security Management

Cybersecurity Basics: Electronic Information, Security, and Management

The concept of ***electronic information*** and the management of that information are at the core of effective cybersecurity. Electronic information can be any idea, concept, or data that is represented digitally and electronically processed. Electronic information can be *stored*, *processed*, or *transmitted*.

- *Storage*: Electronic information is stored *(or "at rest")* when it is not being actively used. Often this means the information has been written (recorded and stored electronically) to devices such as hard drives, local servers, or cloud-based storage.
- *Processing*: Electronic information that is being actively used is being processed.
- *Transmission*: Electronic information can be sent from one electronic system to another—whether those systems are physically near each other (and connected physically or wirelessly) or far apart (and connected via the Internet or other means). When information is sent between systems, it is being transmitted.

Each of these states has important security requirements. For example, a voter registration record must be protected when it is at rest in a database (or as a record that has been backed-up for long term redundant storage), while it is being processed – for example, when it is being used to create local poll book – and when it is being transmitted, such as when electronic poll books are transmitted between locations or systems.

Information security can be defined in terms of three, intersecting dimensions: *confidentiality*, *integrity*, and *availability* (often abbreviated as CIA).

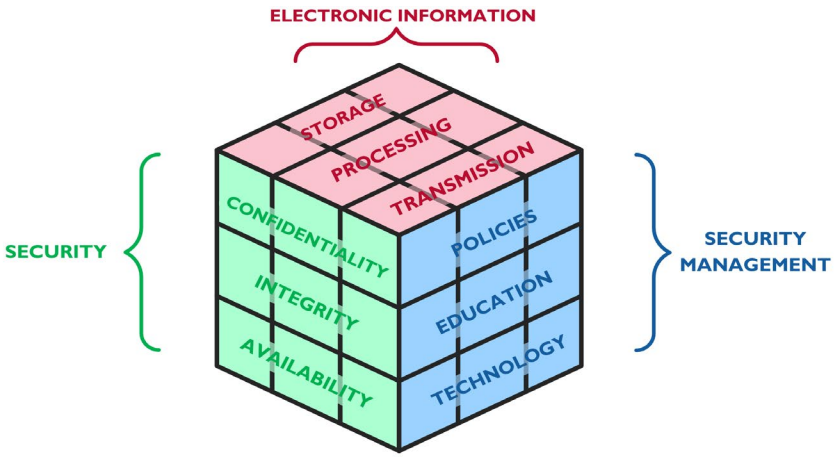
- *Confidentiality* means that information is only accessed by designated, authorized users.
- *Integrity* means ensuring that information that is accessed is not inappropriately altered.
- *Availability* means that information is present and accessible when it is requested.

Information security management maintains the confidentiality, integrity, and availability of information as it is being stored, processed, and transmitted. To achieve and maintain CIA, information security practitioners draw on three broad categories of tools: *policies*, *education*, and *technology*.

- *Policies* can be designed and implemented (for example, password rules or polices defining how information access is granted, to whom and any conditions that may apply);
- *Education* of users, managers, and responsible parties supports and enables effective security (for example, teaching users to recognize signs of malicious intent in emails); and
- *Technology* can be leveraged to help secure and protect information (for example, using encryption to secure transmission of information).

These nine concepts together help to holistically define the process of information security management.[14] Often this is depicted as a cube where all the concepts intersect (shown in Figure 1 below). The intersecting lines help depict the connected nature of information security management across all the discussed dimensions—the information states of storage, processing and transmission must be secured against breaches of confidentiality and integrity, while maintaining availability, through creating and enforcing policies, utilizing technology, and training users and managers.

FIGURE 1: CNSS MODEL OF INFORMATION SECURITY, ALSO KNOWN AS THE MCCUMBER CUBE MODEL.



[14] Over the past several decades, this model has been firmly ensconced within computing security, however for a general overview of the model see: Maconachy, W. Victor, et al. (2001). "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. vol. 310. https://www.researchgate.net/publication/235470635_A_Model_for_Information_AssuranceAn_Integrated_Approach.

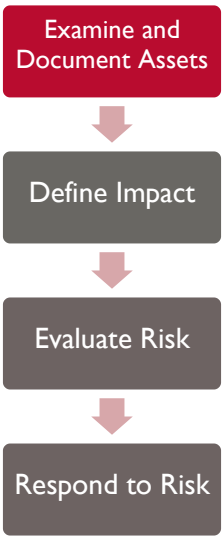
CYBERSECURITY BASICS: RISK MANAGEMENT

Cybersecurity risk management consists of activities that:

1. Allow an organization to examine and document their information technology infrastructure and data (such as computers, network connected devices, software assets, and stored data);
2. Define the impact of compromise or loss of data held by an organization;
3. Help an organization to understand risk as a function of both probability and impact to determine where to invest time and resources; and then
4. Manage that risk with appropriate security controls.

The following subsections examine these activities in turn.

ATTACK SURFACE AND MANAGING INFORMATION ASSETS



A central concept in cybersecurity that is relevant to protecting the electoral process is the **attack surface.** The attack surface of a system or process includes all the ways in which a threat actor can compromise the confidentiality, integrity, or availability of information. The overall attack surface includes both physical and digital threats.

A physical attack surface represents the ways an information asset, such as a computer workstation, server, or other computing hardware, can be compromised by physical access to that device. Various types of equipment are used across election cycles, and each machine or electronic asset has its own physical attack surface. Memory sticks carrying voter registration data may be destroyed, manipulated, or accessed by unauthorized users, or voting machines could be physically tampered with by malicious actors. Protecting against efforts to leverage the physical attack surface is often a matter of physical security. This includes using secure spaces where access is controlled; for example, maintaining equipment in locked data centers or server closets at secured facilities and securing physical ports on computing devices.

The second context is the digital attack surface. This consists of all the ways to achieve access to data, systems and equipment through non-physical means, such as over a network or wireless connection. Electronic transmission of vote tallies could be vulnerable to digital attack, or EMB computers linked to the Internet could be hacked remotely.

An organization's cybersecurity attack surface consists of all possible entry points for unauthorized access into systems both physically and digitally. Often organizations have significant infrastructure connected via the Internet, representing a large portion of an organization's digital attack surface.[15]

[15] For a more formal definition see: NIST Computer Security Resource Center. (n.d.). *attack surface*. https://csrc.nist.gov/glossary/term/attack_surface.

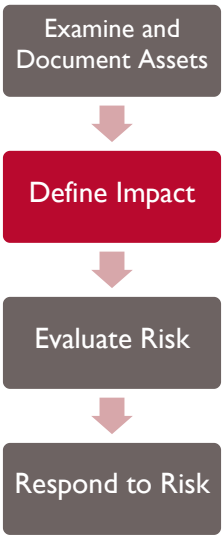
The first steps to understand and manage the attack surface are:

1. inventorying an organization's physical and digital assets; and
2. mapping how they are connected internally and externally.

More specifically, the risk management process should begin by conducting an inventory of hardware, software, and data assets, and understanding how these assets are managed, inclusive of their physical security, on the networks to which they are connected.

EMBs face especially complex asset management needs. Their attack surface may greatly expand during an active election as IT assets are connected and used – for example, at polling stations and as poll workers are onboarded, election equipment is brought online, and voting takes place. This dynamic means that EMBs will need to strategically approach asset management to account for the rapid expansion and subsequent reduction of attack surface. For example: how can new hardware and accounts be rapidly provisioned, without using weak or duplicative passwords or overly broad access permissions, and how can those accounts and permissions be quickly and effectively disabled after the election?

ASSESSING THE "VALUE" OF ELECTORAL DATA



Elections are expensive, cybersecurity threats to elections are significant, and EMBs often face difficult decisions about where to invest limited resources. Before a strategy for securing information can be developed, organizations must define the *value* of the information they control so it can be measured against the cost of security. The value of the information can be defined in strict numerical terms (expressed as a monetary value in some contexts) or it can be a simple ranking across categories. Governments, for example, often employ levels of "classification" ranging from publicly releasable information (that does not adversely impact national security if released) to highly valuable "top secret" information that can cause grave damage if the information is exposed.

It is often difficult to assess the value of data in simple budgetary terms. But understanding the value of information in terms of the operational and mission impact if it is lost or compromised helps inform and balance the security costs of protecting it. Good practices and guidance for making such a determination for election related data do not exist in any great measure. In fact, cybersecurity breaches of election systems may have very different impacts depending on when they occur, how the public interprets the implications of the breach, how election managers respond, and how transparent those response efforts are. EMBs may also control databases that are unique to the electoral context, such as poll worker data or biometric databases, that pose higher risks to privacy should the information leak. Therefore, assigning a value to that impact may be a difficult task that can benefit from more focus and guidance from the broader community of election management bodies and experts.

UNDERSTANDING RISK

Risk is a central concept in information security management. A common model equates risk to the likelihood of something happening multiplied by the impact of that outcome.[16] For example, an EMB may need to evaluate the risks related to maintaining public access for voter registration self-service options accessed via the Internet. The system may be a target for attacks against its availability by overloading the public facing website with so many requests that it becomes unusable. It is reasonable to expect that the *likelihood* of such an attack may increase ahead of high stakes elections and as voter registration deadlines approach. Additionally, the *impact* of such a loss of availability may also increase as various important deadlines approach. Therefore, the risk calculation may change and demand different resources along with different mitigations during various periods of time.

Risk can be further analyzed using the concepts of *vulnerability* and *threat*.

- *Vulnerabilities* are specific weaknesses that exist in a system that an attacker may be able to successfully compromise. Computer vulnerabilities may exist for varied reasons. Most modern software is complex, and that complexity means it is inherently unsecure for reasons that may be known and intentional, or for reasons that may be unknown and due to programming or design weaknesses. Connecting systems to infrastructure such as the Internet allows for diverse benefits, such as making information easily accessible, enabling creative engagement and innovation, or reaching larger audiences. However, these connections also create vulnerabilities that malicious actors can exploit.

- *Threats* are defined as "any circumstance or event with the potential to adversely impact organizational operations through an information system."[17] Understanding who and what may intend harm to an organization and potential threat actors' capabilities is necessary to protect information security.

Overall *risk* is a combination of the likelihood of a threat materializing, how vulnerable your own assets are to that threat, and the consequence of the threat. While there are models that translate each of these pieces into numerical quantities, it is not necessary to think of risk strictly in quantitative terms. Instead, risk can be understood in qualitative terms: ranking threats against each other to understand relative risk.

[16] National Institute of Standards and Technology. *Risk*. https://csrc.nist.gov/glossary/term/risk#:~:text=Definition(s)%3A,likelihood%20of%20that%20threat%20occurring.

[17] This is simplification of the definition that NIST utilizes and can be found here: https://csrc.nist.gov/glossary/term/threat.

FIGURE 2: BUILDING AN UNDERSTANDING OF RISK

RESPONDING TO RISK: SECURITY CONTROLS

There are several industry-standard frameworks that define the risk management process. These frameworks help organizations define and prioritize their security goals and provide sets of actions (putting in place security controls, transferring the risk, or accepting the risk) that can be taken to help address the identified risk.[18]

A security "control" is a measure that can be taken to mitigate a risk. Different frameworks separate controls in different ways, but the following three categories are useful for this discussion:[19] *management controls*, *operational controls,* and *technical controls*.

Security controls can address anything from strategic managerial issues such as articulating and implementing budgetary policies, mandating workforce requirements such as necessary professional certifications, and defining programmatic structure, to very granular controls that address what type of cybersecurity software is used on individual computers, user access rules, and other technical implementation details.

[18] For further information regarding security controls and risk management frameworks, *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document.*

[19] NIST SP 800-53 divides controls into 20 "control families." for security and privacy while ISO27001 utilizes 14 "control sets." The three categories presented here are a general consolidation for the purpose of the present discussion. Another set of commonly utilized controls comes from the Center for Internet Security (CIS) and is divided among 18 categories. See: Center for Internet Security. (n.d.). The 18 CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list/.

FIGURE 3: COMMON CONTROLS

COMMON CATEGORIES OF SECURITY CONTROLS		
MANAGEMENT CONTROLS	OPERATIONAL CONTROLS	TECHNICAL CONTROLS
Management controls are safeguards that use assessments, audits, and planning; e.g. budget planning and other enterprise-wide administrative policies and guidelines.	Operational controls are safety and security measures that are implemented and executed by human beings as they use, interact, and manage electronic information systems; e.g. mandated change management steps, contingency planning, or awareness training.	Technical controls are safeguards that are generally embedded within hardware, software, and firmware to protect information; e.g. encryption, automated monitoring, and use of verifiable security tokens to prove identity.

Establishing security controls is not the only way to manage cybersecurity risk. Risk can also be *transferred;* for example, by sharing responsibilities with other agencies or departments. Within the election space, such risk transference mechanisms may not be easily used or appropriate, depending on, among other things, the type of EMB institutional arrangement or national policies and legal frameworks. Controls also involve defining overarching policies and standard operating procedures for how an organization will respond during cybersecurity incidents.[20] Planning for response and resilience is an integral part of managing cybersecurity risk.

A well-defined cybersecurity risk management process puts in place a holistic strategy, budget, and processes to understand and manage the risk of operating information systems and electronic networks. In the case of electoral administration, for example, the EMB would identify risks, then develop plans to either mitigate or transfer them. If the EMB cannot mitigate or transfer the risks, these risks may need to be accepted.[21] For practical purposes, "accepting" a risk means that an organization formally acknowledges it as a part of doing business – but accepting a risk does not mean it can be ignored, but rather that is understood, minimized, and actively monitored. For example, an EMB may decide that the risk of interconnecting their systems with a government ministry is necessary to support essential function despite that ministry not adhering to the same security controls or risk posture as the EMB. Accepted risks should be identified and tracked within a "risk register." Risk registers are continuously updated as new risks are identified and others retired, which occurs when controls are developed and applied to mitigate known risks, or when risks are eliminated.[22] Securing organizations and complex enterprises against cybersecurity threats is a complicated endeavor requiring strategic approaches.

Following standard industry protocol, EMBs should use a formalized risk management framework that creates a rigorous, repeatable process for identifying, tracking, and minimizing risk over time.

[20] The particulars of which are also not defined nor developed within the present discussion.

[21] Not discussed here are the granular actions that operationalize the high-level process. This includes the use of specific plans, sometimes referred to as "information system security plans," that help organize the implementation of controls on and across discrete information systems and networks.

[22] It should be noted that often applied security controls can only sufficiently mitigate a portion of the risk present with the operation of any specific information asset or associated process, the "left over risk" that is uncontrolled is characterized as "residual risk" that must be recognized and deemed acceptable or rejected. This residual risk is also defined and tracked within the risk register.

Section IV: Cyber Risks for Electoral Processes and Assets

As more countries digitize their electoral processes,[23] they may be exposing an increasing amount of their electoral infrastructure to risks, creating new possible vulnerabilities to threat actors. Understanding which processes are most at risk for a given EMB or electoral environment can be difficult given the sheer variety of different contexts across various countries and regions. However, a review of recent trends indicates that EMBs and their partners may face challenges protecting voter registration databases and results tabulation and transmission systems. These systems often include elements accessible via the Internet, making them attractive targets for cyber attacks that undermine stakeholder acceptance of electoral outcomes.[24] Cyber risks can be further compounded by poor cyber hygiene[25] among institutions and users involved in administering and maintaining election technology; and by *ad hoc* and piecemeal approaches to cybersecurity involving third parties, technology procurement and multi-stakeholder collaboration that makes holistic cybersecurity management difficult or impossible.

It is important to consider the attack surface of each process and system involved in electoral processes with regards to confidentiality, integrity, and availability. Voter register databases and functions can increasingly be accessed online by members of the public — either to simply check registration status, or to execute voter registration or absentee ballot requests. This ease of access represents an expansion of the attack surface and the benefits of these tools must be balanced with the risk that such resources may be compromised by malicious actors undermining election processes. Other processes such as results transmission systems may rely on sending information over the Internet and should be sufficiently encrypted and protected. Sending results data via physical media such as USB drives can also be subject to interception and should be protected in transport and be checked for integrity.

Particularly during the campaign and period of lead up through an election itself, many EMBs will not be able to address escalating cyber attacks on their own. Information technology is used across the entirety of an election cycle, and is owned, maintained, and used by a variety of actors – from software and hardware providers to candidates and other institutions that play a role in election administration. Yet, because the activities performed across the electoral process are interrelated, security compromises or breaches with one involved stakeholder can have wide-reaching effects. Often EMBs must interact with or depend on other state institutions; for example, they may access national ID databases when verifying voter registration.

---

[23] For information about specific technologies used in elections see IDEA ICT in election database (n.d.). https://www.idea.int/data-tools/question-view/739

[24] USAID. (2022). Understanding Cybersecurity Throughout the Electoral Process: A Reference Document

[25] Cyber hygiene is a term that is used to indicate the body of good practice that users of information systems should utilize in order to keep themselves and their data safe and secure. This includes using strong authentication, looking for indications that a link could be dangerous to click on, not plugging in unknown USB hardware, and other such practices. Cyber hygiene can also extend to good managerial practices, such as mandating user education, auditing and assessing user adherence to good practice, and remediating or mitigating cybersecurity issues that are found.

Therefore, cybersecurity should be addressed holistically throughout electoral infrastructure and related interfaces. EMBs will need to work with other stakeholders. This may include state offices that compile civil registries from which voters lists may be pulled or authorities auditing voting machines, to establish mature cybersecurity postures across the entire electoral process. It is necessary to begin this process well in advance of the election itself, to establish the relationships to coordinate and respond to real-time incidents.

RISK ANALYSIS

Although risk analysis is inherently subjective, this section offers a framework for categorizing and prioritizing cybersecurity risks in various parts of the electoral process. This analysis considers past cyber attacks globally – both generally, and on elections in particular – and assigns two values to each part of the electoral process, represented in the matrix below: ***potential for exploitation*** and ***impact on electoral integrity***.

"Potential for exploitation" is deemed to be *higher* if: 1) the process commonly involves a public facing component that is accessible via the Internet; 2) vulnerabilities specific to the common information technology used for that process have been identified; and 3) the process has been a target of attacks, as informed by available reporting and analysis. If a process has public facing components but reports of it being targeted outside of proof-of-concept demonstrations have not been found, it is judged to have lower potential for exploitation *currently*. This is not to say processes appearing in this category won't be at risk in the future.

Processes assigned to the ***"higher impact"*** category are assessed as likely to undermine electoral integrity more rapidly than those listed as lower impact. While this is an oversimplification of the risks to longer term electoral integrity, it should provide a reasonable starting point to identify the risks most likely to result in significant and potentially irreversible impact before a response can be mobilized. Exploitation of processes such as election dispute resolution and candidate registration can conceivably be detected and corrected before significantly impacting electoral integrity. In contrast, exploitation of processes such as results transmission, tabulation, and reporting may result in larger impacts to electoral integrity and public trust due to the shorter timeframes for detection and mitigation, possibly calling into question election outcomes. The estimates of impact in the following risk matrix and analysis seek to combine these factors.

A further note on impact and assessing risk in your local context: As noted above, impact cannot be fully assessed based on a single criterion such as rapidity. Each of the electoral processes represented in the risk matrix below – from voter or candidate registration to results tabulation – can be implemented using a variety of technologies in operationally diverse ways - and managed well or poorly. The real-world impact of an attack or compromise of one of these systems therefore depends on many external factors including, for example:

- The technical maturity of a country's overall cybersecurity response infrastructure
- The level of technical and operational redundancy within each component of electoral process
- The transparency and quality of response measures following a cybersecurity incident
- Level of public trust in election infrastructure, EMB, and the electoral process more broadly

In the cybersecurity industry, risk ratings are often determined by subject matter experts who weigh the importance of a system to the specific business or mission outcome that it supports along with other factors unique to the specific implementation. Discussions among relevant experts are then translated into some form of qualitative or quantitative scoring for making managerial and resource decisions on how to either eliminate, mitigate, accept, or otherwise manage the risk. These approaches are highly context specific. For example, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has developed tools that help local U.S. state election administrators integrate their knowledge of their local systems and process to understand impacts of possible compromise. The CISA tool helps administrators prioritize their cybersecurity efforts and budgets by helping local election administrators rank risk to systems relative to each other. [26]

Similarly, with additional local context, the risk matrix below can serve as a starting point to help DRG officers and EMBs categorize relative risk among electoral processes. Readers of this primer should apply evaluations of local context to each electoral process to understand how to approach impact and potential for exploitation specific to the country under examination. **This may result in various processes being categorized very differently than how they appear on the illustrative risk matrix seen in Figure 4.** For example, a country that has a mature national digital identification program that is leveraged during the voter registration process may not assess risks associated with voter data databases with public facing components with the same urgency as it appears to necessitate in Figure 4 below. Countries with immature or new digitization efforts may present very different risk profiles based on factors related to how such efforts have been implemented.

FIGURE 4: ILLUSTRATIVE ELECTORAL PROCESS RISK MATRIX

	LOWER POTENTIAL FOR EXPLOITATION	**HIGHER POTENTIAL FOR EXPLOITATION**
HIGHER IMPACT	• Boundary Delimitation • Voting and Counting Processes	• Voter Registration • EMB Communications • EMB-led Voter Information and Education • Results Transmission, Tabulation, and Reporting
LOWER IMPACT	• Electoral Dispute Resolution Process	• Candidate Registration Process

[26] While developed for and particular to the U.S. elections system, CISA's Election Security Risk Profile Tool helps illustrate how local context is necessary when evaluating impact. To use the tool, local (municipal level) election administrators are asked to assign qualitative impact ratings using their expertise over their local systems and processes. The tool itself may not be useful to non-US contexts, but reviewing the tool's documentation and the Election Security Resource Library offered by CISA can help understand what sort of granular local context and information is useful for understanding election risk rating. For the tool see, CISA. *Election Security Risk Profile Tool: How to Use.* (n.d.). https://www.eac.gov/app/esa/how-to-use and for further resources see, CISA. *Election Security Resource Library*. (n.d.). https://www.cisa.gov/election-security-library

HIGHER POTENTIAL FOR EXPLOITATION – HIGHER IMPACT

KEY ASSETS AT RISK:

- Databases, both EMB and from other national entities (e.g., national ID, passport, civil registry)
- Data storage devices (e.g., USBs, external hard drives)
- Voter PII and biometric data
- Varies by country

Voter Registration

Voter registration databases present an attractive target to threat actors. Voter registration (VR) processes rely on databases that store and manage voter registry data, as well as digital components and processes related to registering voters. At their core, all voter registration systems are structured as databases that contain voters' personally identifiable information (PII). The degree of automation, the type of data, and the range of services varies depending on a country's legal framework and the election administration's eagerness to deploy new technologies. These types of databases have been breached in multiple countries and represent a high potential to attract further attacks that can degrade public confidence in the electoral process.

The attractiveness of voter registration data to threat actors may be increasing as countries use biometric devices to capture fingerprints, iris scans,[27] and digital photos. These three forms of biometrics are unique to every individual, and it is these unique features and other personal details that will be stored in the computer from which the voter register is produced. The main benefit of biometric voter registration (BVR) is its ability to detect and flag, as well as deter, multiple registrations. Biometric data is also used to identify voters at polling stations,[28] and network-connected biometric verification devices can be used to prevent an individual from casting a ballot at multiple locations on election day.

However, both PII and biometric data can potentially be used for other malicious purposes such as identity fraud or to execute targeted disinformation campaigns, or even for targeting individuals for surveillance. Direct manipulation of voter registration data – for example, adding or deleting voters – also cannot be ruled out as a possibility if voter registration database security is compromised.

EMB Communications and Voter Information and Education

Both EMB external communications and voter information and education processes present a high potential for exploitation that can have a significant impact on electoral integrity.

KEY ASSETS AT RISK:

- EMB email systems
- EMB websites
- Social media accounts

The systems EMBs use to communicate with the public, such as websites, social media, telephone, and other public facing infrastructure, should all be considered potential targets. For example,

[27] Though less common than fingerprints and digital photos, Somaliland and Puntland have both used iris scans successfully in recent elections. For information about their use in Somaliland see: Report by International Observers on the 2016 Voter Registration Process in Somaliland, Marie-Luise Schueller and Michael Walls, University College London (UCL). IFES assisted the Transitional Puntland Electoral Commission (TPEC) in evaluating voter registration options and designing its voter registration solutions for the 2021 local council elections. In the end, TPEC used a combination of biometric data, including iris scans. For further details, see https://tpec.pl.so.

[28] IDEA ICT in election database (n.d.). - https://www.idea.int/data-tools/question-view/739

EMB social media accounts have been compromised and then controlled by threat actors to mislead the public, resulting in confusion or suppressed voter turnout.[29]

These kinds of attacks often do not require technical sophistication or significant funding and can additionally be appealing because they are often difficult to attribute after the fact. Beyond compromising existing accounts, disinformation tactics can be employed, such as impersonating official entities and senior officials through fake social media accounts also leading to confusion and potentially affecting electoral integrity.[30]

Malicious actors can also affect result reporting, when the voters and citizens are most keenly awaiting information, by compromising official results reporting websites and communications channels. For example, North Macedonia's State Election Commission's official website was attacked shortly after the end of an election in July of 2020. This prevented "…journalists and other interested people from monitoring the election results, which were announced with a huge delay a day after the election."[31]

Results Transmission and Tabulation

Attacks on results transmission and tabulation systems are a common – and long-standing – tactic for actors seeking to undermine trust in elections.[32]

KEY ASSETS AT RISK:

- USB memory sticks
- Hard drives
- Telephone based transmission systems
- Official websites and associated infrastructure

Actors perpetrating such attacks may seek to alter vote counts or create public confusion and doubt about the integrity of an election outcome. Distributed Denial of Service (DDoS) attacks (discussed further in the next section) may also be staged at this phase of an election - preventing public access to results sites by overloading them with requests. Along with attacks on elections systems and websites, disinformation campaigns pose a major threat in the post-election period. Release of false

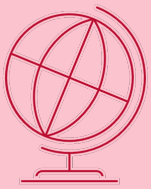
[29] In Cambodia in 2017 for example, the Facebook account for the Spokesman of the National Election Commission (NEC) was hacked and controlled by outside actors "for weeks," preventing accurate flow of information between the NEC, media and public. See Phnom Penh Post. (2017, October 9). *NEC Facebook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

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

[31] Dimitrievska, Valentina. (2020, July 19). *Who hacked the website of North Macedonia ' s state election commission on election day?*. https://www.intellinews.com/who-hacked-the-website-of-north-macedonia-s-state-election-commission-on-election-day-187756/

[32] For the South African system was compromised in 1994, see: Harris, P. (2011). *Birth: the conspiracy to stop the'94 elections*. Penguin Random House South Africa.

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



One of the most prominent examples of an electoral cyber attack occurred during the 2014 presidential election in Ukraine, which followed the country's Revolution of Dignity and the subsequent invasion of Donbas by Kremlin-supported forces. The attack consisted of multiple parts. Four days before the national vote, malware was planted on Ukraine's Central Election Commission (CEC) servers that rendered the vote tallying system inoperable and could have altered election results. The system was restored using backups.

On the day of the election, a DDoS attack on the Ukrainian CEC shut down its website for a time. In the meantime, a Moscow TV station, broadcast an election results website purporting to be that of the CEC that showed the election was won by a minor pro-Russian candidate. Upon seeing this, the CEC immediately began reviewing its own website and found that a fake image of inaccurate results, like the one displayed by RTI, had been placed on the CEC servers. If undiscovered, the image would have been displayed instead of accurate results when the polls closed at 20:00. As the data underlying it was not connected to the website, the CEC was able to restore the correct results on its website and fix the underlying vulnerability 40 minutes ahead of the deadline. The incident brought into sharp relief the damage that could have been done to the integrity of a pivotal election, had the attack not been detected in time. [33]

LOWER POTENTIAL FOR EXPLOITATION – HIGHER IMPACT

Voting and Counting Processes

In Figure 4, the voting process is shown as being at a lower level of potential for exploitation. This is because, while proof-of-concept hacks of ballot casting devices have been demonstrated, they have not been followed by widely reported instances of confirmed vote manipulation, at the time of this writing. However, the potential impacts of such threats should not be underestimated and can range from sowing confusion due to malfunctioning devices to manipulation of voting and manipulation of vote totals. Politicians and malicious actors have fed and encouraged public perceptions of more widespread prevalence of such manipulation. On election day, a variety of technologies may be used for authenticating voters, casting votes in

KEY ASSETS AT RISK:

- Biometric authentication devices
- Electronic voting machines
- Ballot scanners
- Internet voting infrastructure

[33] Ukrainian parliamentary election interference (2014). (2021, July 6). International cyber law: interactive toolkit. Retrieved 19:52, March 3, 2022 from https://cyberlaw.ccdcoe.org/w/index.php?title=Ukrainian_parliamentary_election_interference_(2014)&oldid=2435; also see Martin-Rozumilowicz, B. and Chanussot, T. (2019, October). Cybersecurity and Electoral Integrity: The Case of Ukraine, 2014-present. In Krimmer, R., Volkamer, M., Beckert, B., Driza Maurer, A., & Serdült, U. Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019: 1-4 October 2019. (278-292). Lochau/Bregenz, Austria: Proceedings. https://www.zora.uzh.ch/id/eprint/175950/1/Krimmer_et_al_E-Vote-ID_2019.pdf

polling stations, and counting votes such as electronic or biometric voting authentication, optical scanners to automate ballot tabulation and reporting, ballot marking devices, and direct recording electronic (DRE) voting machines.

DRE machines have been shown to be vulnerable to various types of potential attacks, including man-in-the-middle attacks (see section VI), which seek to change information or votes.[34] These have been successful in controlled attempts both within the United States and the Netherlands, and to some extent, their success has also led to a significant adjustment or roll-back of this technology in these and other countries. While there are not many examples of successful attacks in the real world on the balloting process, it is important to continuously evaluate new data as it emerges to understand if threat actors may be better positioned to compromise the voting process itself in the future; such new information would mean the potential for these attacks would move from lower to higher.

The danger for electronic voting machine (EVM) manipulations does not only stem from the machine's software, but also the hardware. Supply-chain risk management, discussed further below, has become a major concern following a recent increase in globally-reaching attacks.[35] If a threat actor can gain access to an EVM while it is being transported or assembled, for instance, there are several ways the machine may be altered to facilitate vote manipulation.[36] A device could be inserted to take control of the unit, a chip that records the votes could be replaced with a fraudulent or malicious chip, or the software could be compromised before it is installed in the EVM to alter votes after they are entered but before they are recorded, or other malicious impacts are possible through such hardware manipulation.

It should also be noted that, though it varies among regions, countries, and localities, EMBs may not always have adequate technical staff to service fielded equipment. Often, they are only able to deal with problems in urban areas due to distance and number of trained IT personnel. If the technology is recently introduced, the training of EMB's IT support teams is done by the vendor. In other instances, the vendor is supposed to offer that type of IT-support on behalf of the EMB, which may increase risks of insider attacks (see section VII) among other issues.

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

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

[36] Hodgson et al. (2020)

In 2018, Iraq began using ballot scanners that were expected to transmit results through the mobile phone network. Outside mobile phone coverage areas, the results of those ballot scanners were loaded on USB memory sticks and physically transported to regional results centers. Several such USB devices were reportedly intercepted and manipulated. The results data was changed, so that it no longer aligned with the scanned ballots in the ballot box.[37]

Global interest in and demand for Internet voting has increased with the COVID-19 pandemic. The technological infrastructure for Internet voting is probably one of the most difficult an EMB can choose to implement. Internet voting provides an opportunity to resolve some historical inclusion challenges – such as enfranchisement of voters abroad, women who might not be able to leave their homes or are not able to vote at polling stations with men, voters with disabilities and internally displaced persons. However, it also introduces a wide range of new risks and concerns from the perspective of confidentiality, integrity, and availability of the election systems and results. Security – as well as public perception of security – should be a key consideration before implementing Internet voting. Several countries have moved away from limited Internet voting programs – including the Netherlands and Norway – over security concerns by voters and election administrators. [38]

Boundary Delimitation

KEY ASSETS AT RISK:

- GIS systems and associated databases, including online portals used to share GIS information with political parties, observers, and voters
- Connected systems at related institutions (e.g., census institution, ministries responsible for national cartographic services)

The boundary delimitation process refers to drawing electoral district boundaries (or constituencies). It also involves determining electoral precincts and polling locations and assigning voters accordingly.[39] Technology has been increasingly integrated into these processes to precisely map locations and distribute voters, replacing mostly cumbersome manual systems. There have not been any reported attacks against the electoral process using boundary delimitation tools or access. Therefore, this process is categorized in Figure 2 as having lower potential for exploitation. It is categorized here as potentially high impact, however, due to the foundational nature of boundary delimitation within the overall electoral process. Successful attacks against boundary delimitation systems or processes could, for example, gerrymander precinct boundaries in favor of one party or

[37] European Union Election Expert Mission to Iraq. (2018). *Final Report (5 April – 31 May, 24-31 July 2018).* European Union; and Wahab, B. (2018, June 11). *Recount will Test the Integrity of Iraq's Elections*. Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/recount-will-test-integrity-iraqs-election

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

[39] Handley, L. (2007). "Boundary Delimitation." In *Challenging the Norms and Standards of Election Administration*, International Foundation for Electoral Systems. 59-74.

another. Because the number of locations and accessibility of voter registration sites are often based on boundary delimitation data, a successful attack could also impact the practical ability of targeted communities to register and subsequently vote. Furthermore, even if such attacks were detected prior to election day, correction of the data could be expensive and time consuming, which itself might make the subsequent electoral processes unachievable.

These systems may be vulnerable if data sources they draw from are externally facing and connected to the Internet (such as geographic information systems databases), or if they are interconnected to other state institutions, such as census institutions or ministries. Geographic Information Systems (GIS) and associated services are often procured rather developed in-house, potentially exposing the process to supply chain vulnerabilities in the case that vendor procured systems or services are themselves compromised. As discussed earlier, impact should be evaluated within the local context to determine impacts and risk particular to a country or implementation.

HIGHER POTENTIAL FOR EXPLOITATION – LOWER IMPACT

Candidate Registration

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

KEY ASSETS AT RISK:

- Online registration websites
- Physical registration sites including biometric information capture devices
- Candidate information databases
- Communications systems (e.g., email or dedicated registration information transmission systems, official websites where candidate information is posted)

Although some of this information may be appropriate to disclose in the public domain for the sake of transparency, other data may be targets of manipulation or identity theft. As such, categories of data should be clearly delineated by the EMB and sensitive data should be protected. This personal information may become a target for various malicious actors seeking to steal information for political purposes or financial gain.

Where electronic registration mechanisms are used, the information that is printed on election ballots is often derived from the registration system. Ballot errors (or manipulations) can lend prima facie grounds for election annulment, hence making for an attractive cyber target. As candidate registration often occurs ahead of elections on timescales that allow for scrutiny, while a risk – the process is considered lower risk since the issue can potentially be recognized and corrected before impacting electoral integrity. Again, impact should be further evaluated using local context. For example, in cases where an online candidate registration system is used to gather details such as a candidate's full name, photograph, and party information that is then used to create printed ballots, the potential for a well-timed attack that prevents printed ballots from being produced correctly could be grounds to move this to a higher impact category. Often elections involving many candidates drive complex ballots utilizing a number of designs. As a result, errors do occur despite EMB quality checks and this makes intentional manipulation a possibility that cannot be discounted.

LOWER POTENTIAL FOR EXPLOITATION – LOWER IMPACT

Election Dispute Resolution

KEY ASSETS AT RISK:

- Online EDR complaint portals
- Other systems connected to the EDR process

Effective resolution of electoral complaints is essential to the integrity and legitimacy of an election. Increasingly, election dispute resolution (EDR) bodies use technology as part of the complaints adjudication process. For example, many forums accept complaints through online channels, some online portals allow the uploading of electronic evidence, hearings are increasingly being held remotely, and EMBs and EDR tribunals also increasingly rely on electronic case management systems.[40] These EDR systems have public facing components and may contain sensitive data related to electoral contests (e.g., candidate information, voter registration data, and election results data). Attacks against EDR systems can result in reputational impacts and could affect public perception of the overall process.

Cyber attacks on the EDR process may not currently be considered as high of a risk to electoral processes as attacks on other core EMB systems, such as voter registration or the ballot casting process based on reported incidents. However, any malicious actor seeking to manipulate or undermine electoral processes would be aware of *all* public facing systems that could be easily taken offline or manipulated. Therefore, EDR bodies, and particularly those confronting the likelihood of close or contested elections, should take many of the same risk mitigation steps that EMBs and other electoral stakeholders take to protect their systems from cyber attacks.

Section V: Types of Cyber Attacks and Related Tactics

As discussed earlier, cyber attacks make use of vulnerabilities in software, hardware, process, and human behavior that can be exploited to compromise the confidentiality, integrity, or availability (or any combination therein) of information in electronic systems. Cyber threat actors—the entities or individuals that seek to attack these systems—make use of many different tactics, techniques and procedures (TTPs). The TTP framework is broadly used by the security community to define the universe of techniques and associated actions malicious actors employ to achieve their intentions.

TTPs are important to consider as, often, certain mixes of techniques, tactics, and procedures can distinguish particular threat actors from others. While TTPs specific to cyber attacks directed at elections have not been defined, the broader concept is still important to help distinguish among various threat actors. In addition, cybersecurity practitioners use a comprehensive understanding of TTPs to put in place the controls that are best able to provide defense across the information infrastructure they are trying to secure. The discussion of cybersecurity TTPs can easily extend into granular technical dimensions; this primer will only provide an introduction of how various threat actors employ and favor specific methods, tools, and actions.[41]

---

[40] Davis-Roberts, A. (2009, January). *International Obligations for Electoral Dispute Resolution: Discussion Paper*. The Carter Center. https://www.cartercenter.org/resources/pdfs/peace/democracy/des/edr-approach-paper.pdf

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

While cyber attackers make use of a large variety of tools and methods, understanding common elements that many attacks evince is helpful. One useful distinction is between *untargeted* and *targeted* attacks.[42] Untargeted attacks are indiscriminate in terms of who or what is being exploited, whereas targeted attacks single out specific systems, users, or entities.

UNTARGETED ATTACKS: COMMON TECHNIQUES [43]	
PHISHING	Tricking users into disclosing sensitive information such as usernames and passwords or tricking users into allowing malicious software to be downloaded and deployed. This is often done by sending out a large number of emails or other communication (such as text messages or other messaging applications) designed to trick users into clicking on malicious links or responding with sensitive information. This attack is considered un-targeted when attackers distribute phishing attacks widely.
WATER HOLING	This type of attack uses fake websites that may emulate a legitimate website or seem to serve a legitimate purpose but is in fact a way for malicious actors to exploit users. Sometimes attackers set up websites that look similar or identical to something legitimate companies or governments utilize.
OPEN SCANNING	Scanning a large swath of the Internet looking for vulnerabilities to exploit.

Targeted attacks, on the other hand, single out specific systems or users:

TARGETED ATTACKS: COMMON TECHNIQUES[44]	
SPEAR PHISHING	This type of attack, like phishing, tries to trick users into disclosing sensitive information; however, spear-phishing is a far more targeted variant of the technique. Often nation states and sophisticated actors will tailor the content of email or the way information is presented, to make it more likely the target will be tricked based on intelligence and specific information about that individual or entity.

[42] This distinction and the following discussion of attack stages is synthesized from the United Kingdom National Cyber Security Centre (NCSC) Information webpage. The NCSC bases this on Lockheed Martin's Cyber Kill Chain model. For the simplified UK cyber attack model see United Kingdom National Cyber Security Centre (UKNCSC). (n.d.). *How cyber attacks work*. https://www.ncsc.gov.uk/information/how-cyber-attacks-work; and for more information regarding Kill Chain see: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[43] Ibid.

[44] Ibid.

TARGETED BOTNET OPERATIONS	Botnets are collections of Internet connected computers that have been compromised and consolidated under the command and control of a malicious threat actor. Often criminals will rent their command and control infrastructure for targeted attacks against specific websites and online entities. The resulting Distributed Denial of Service (DDoS) attack results in a loss of availability as targeted websites become overloaded with requests and are inoperable.[45]
SUPPLY CHAIN ATTACKS	Supply chain attacks compromise hardware and software components, not at the point of use but at some stage prior. For example, inserting a hardware modification or software vulnerabilities during or after the manufacturing or software engineering process, but before the product has been integrated into an EMB's IT infrastructure. The recent breach of software company SolarWinds is an example of this type of attack. A threat actor compromised SolarWinds' software update process, and since SolarWinds software was used widely by other companies to monitor their own networks, threat actors were then able to compromise the networks of entities that utilized the SolarWinds software update.[46] Supply-chain considerations also include identifying and vetting trusted providers that are transparent and can ensure their products do not incorporate untrusted or compromised components.

Other common tactics and techniques include the following that have both targeted and untargeted uses:

OTHER COMMON TECHNIQUES	
SOCIAL ENGINEERING	Social engineering often relies on means that are not technological in nature but rather exploit human nature to gain sensitive information that can be used to compromise electronic systems. Examples of this include criminals posing as customer service representatives over the phone and tricking targets into disclosing sensitive passwords and PIN numbers.
MAN IN THE MIDDLE	Man-in-the-middle (MitM) attacks consist of intercepting communications between users and a legitimate destination to read or change the communication before relaying the information onto the destination, without having compromised the destination website or system.
RANSOM WARE	Often the techniques discussed above are leveraged to compromise networks to deploy software that encrypts the data on target systems in a type of attack termed *ransomware*. Threat actors may then contact the victim and offer to decrypt their data for a fee. Such a tactic can also be utilized for destructive attacks that cause deletion of information or other negative effects.

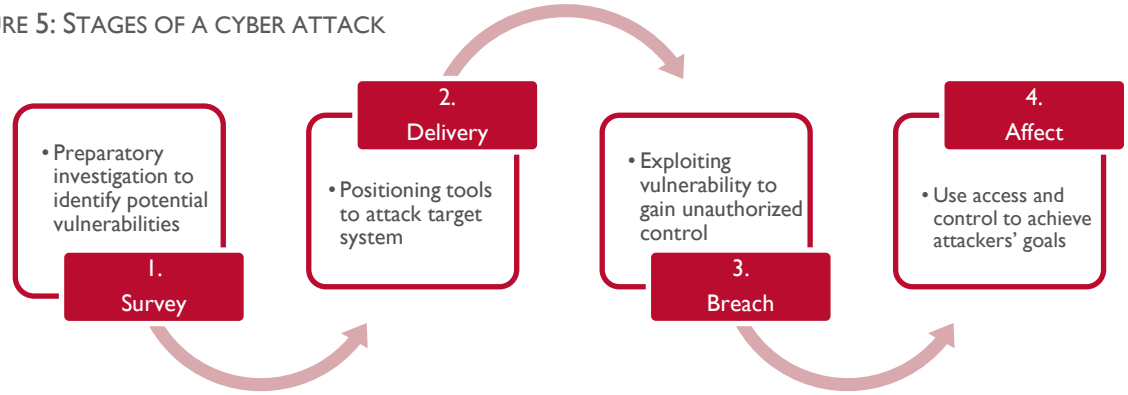
[45] See for example the various DDoS attacks against the Ukrainian Central Election Commission detailed in Martin-Rozumilowicz (2019 October).

[46] For background on the Solar-Winds breach, see United States Cybersecurity & Infrastructure Security Agency. (n.d.). *Supply Chain Compromise*. https://www.cisa.gov/supply-chain-compromise

INTERCEPTION AND COMPROMISE OF PHYSICAL DEVICES	This is a tactic that is frequently encountered at the transmission stage of the voter registration process, when registration data has been loaded onto physical media for transportation to national centers for aggregation. Stealing devices for their intrinsic value is common, Laptops or hard drives can be easily resold on the black market. Instances have been reported in Hong Kong[47], the Philippines[48], Malawi[49], Canada[50], and the US (Atlanta).[51] Access to the physical devices where the data is stored may allow malicious actors to manipulate the list to add names either manually or with some automation. Specially crafted malware can be developed and injected via USB allowing for further manipulation. Access to the voter registration machines, even for a few seconds, can then compromise the integrity of the list. In most extreme cases, if the disruption of the election operation is the ultimate objective, actors might choose to simply destroy the devices and/or their content.

Most attacks against information systems follow a series of common actions or "stages"[52] like the ones depicted in the simplified version of a standard model of cyber attack featured below.[53] A well-developed cybersecurity risk management program intentionally designs security controls to help ensure attacks are recognized and prevented in early stages, but also makes sure to include security controls that help detect, respond, and if needed, recover from attacks that have progressed to later stages. In this sense, cybersecurity should not be thought of only as preventive measures but should also include well thought-out mechanisms to address attacks that have progressed past initial stages.

FIGURE 5: STAGES OF A CYBER ATTACK



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

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

[49] Sangala, Tom. (2018, October 30). Voter registration 'kit' stolen. *The Times Group.* https://times.mw/voter-registration-kit-stolen/

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

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

[52] United Kingdom National Cyber Security Centre (UKNCSC). (n.d.). *How cyber-attacks work.* https://www.ncsc.gov.uk/information/how-cyber-attacks-work.

[53] Ibid.

A note on disinformation: While not comprehensively addressed in this primer because it is not a cybersecurity issue, one additional technique worth highlighting is the use of disinformation about election technologies. Disinformation is often used to undermine public confidence in the electoral process or for other motives. Politicians in developing countries have long sought to blame election technology vulnerabilities for their electoral defeats. This trend has more recently been seen in both emerging democracies and in the developed world — both in the pre- and the post-electoral context. In the United States, the fallout of such actions has led to multi-million-dollar lawsuits by the election technology industry[54] and has reportedly eroded public confidence in elections among large segments of the electorate.[55] While it remains true that election technology cannot be completely protected against cyber threats, the lines between hypothetical vulnerabilities and successful cyber attacks have blurred in the public consciousness.

Section VI. Threat Actors and Possible Motivations

Election infrastructure has been targeted by a variety of threat actors with different motivations. The following section presents five types of threat actors based on the tactics and techniques they apply and their apparent motivations and aims.

1. Foreign State Actors and Advanced Persistent Threats

Malicious actors associated with or directly tied to foreign governments constitute a grave threat to election security. Assessing the objectives and motivations of such actors can be difficult; however, there is general consensus among analysts that many malicious foreign actors are seeking to undermine democratic institutions and sow political discord.[56] The Kremlin's motivations, for example, are assessed by some analysts to be focused on generally undermining democratic institutions while the People's Republic of China may be using a more targeted approach to influence specific foreign policy goals and interests.[57] Malicious threat actors associated with foreign governments are generally well-resourced and utilize sophisticated techniques. This level of sophistication is described by the term "Advanced Persistent Threat" or APT, and there are different industry and government designations for important APT threat actors.

Among actors that can sustain and execute cyber operations at the APT level, two - designated APT 28 and APT 29 respectively - are worth discussing further. APT 28, also known within the industry as "Fancy Bear," is part of Kremlin's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service

[54] Dean, G. & Shamsian, J. (2021, August 14). From Mike Lindell to OAN, Here's Everyone Dominion and Smartmatic are Suing over Election Conspiracy Theories So Far. *Business Insider*.
https://www.businessinsider.com/everyone-dominion-smartmatic-suing-defamation-election-conspiracy-theories-2021-2?op=1

[55] Laughlin, N., and P. Shelburne. (2021 January 27). *How Voters' Trust in Elections Shifted in Response to Biden's Victory.* Morning Consult. https://morningconsult.com/form/tracking-voter-trust-in-elections/

[56] For the American context see recent U.S. Director of National Intelligence report: National Intelligence Council. (2021, March 10). *Foreign Threats to the 2020 US Federal Elections*.
https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

[57] Hanson, F., S. O'Connor, M. Walker, and L. Courtois. (2019). *Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections*. International Cyber Policy Centre. https://apo.org.au/node/236546

Center.[58] APT 29, also known within the industry as "Cozy Bear," is attached to the Russian Foreign Intelligence Service (SVR).[59] Both groups have been responsible for some of the highest visibility and most effective cyber operations against elections entities over the past several years.[60] Identifying operations carried out by APT 28 and APT 29 relies, in part, on assessing the TTPs they typically utilize.

These operations are characterized by sophisticated methods that make use of "zero-day exploits" to gain and sustain access to information systems. Zero-day exploits are so named since they take advantage of vulnerabilities that the larger cybersecurity industry is not aware of and therefore cannot be easily defended against. A recent example is the Apache Log4j vulnerability. Log4j is a widely-used software utility that can be integrated into other software projects by developers to log certain types of information to help in debugging and troubleshooting software issues. In November 2021, an individual working for an international company's security found and publicized that Log4j contained a vulnerability that could be leveraged to access some of the systems in which it was used. This vulnerability was previously unknown, making it a "zero-day" exploit.[61] Due to Log4j's widespread usage, the US Cybersecurity & Infrastructure Security Agency (CISA) along with other relevant global cybersecurity agencies and experts labeled the vulnerability as representing a clear and present risk, advising mitigations be immediately put in place and security updates be made to affected systems. APT 28 and APT 29 have access to a large supply of zero-days, which highlights their relationship to government resources; such exploits require sustained research and experimentation to identify. This is known to be the case based on the number of previously unknown exploits found to have been used by those entities when investigating breaches by those threat actors.[62]

In addition, these well-resourced groups can use their state-level intelligence relationships to engineer sophisticated spear-phishing operations targeting high value individuals (in the election arena, this may include, for example, EMB commissioners and key IT personnel, current incumbents or candidates for high-level office and the leadership of major political parties). APT level threats use sophisticated intelligence and reconnaissance techniques to craft these operations in a way that makes it hard for victims, even persons that have had training, to distinguish malicious content from legitimate communications. APT 28 and 29 have operated since the mid-2000s and their efforts have often been geopolitically targeted at undermining the credibility of democratic and, later, electoral systems, therefore posing a considerable threat to public trust. The People's Republic of China, Iran, and North Korea all have sophisticated offensive cyber operations that leverage APT level tools, tactics, techniques, and procedures.[63]

---

[58] Mitre Att&ck. (n.d.). *APT28*. https://attack.mitre.org/groups/G0007/; and Crowdstrike. (2021, April 1). What is an Advanced Persistent Threat (APT)? https://attack.mitre.org/groups/G0007/ and https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[59] Mitre Att&ck. (n.d.). *APT29*. https://attack.mitre.org/groups/G0016/

[60] Burgess, M. (2017, November 1). Exposed: How One of Russia's Most Sophisticated Hacking Groups Operates. *Wired Magazine*. https://www.wired.co.uk/article/how-russian-hackers-work

[61] United States Cybersecurity & Infrastructure Security Agency. (n.d.) *Apache Log4j Vulnerability Guidance*. https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

[62] Burgess (2017)

[63] Mandiant. (n.d.). *Advanced Persistent Threat Groups.* https://www.mandiant.com/resources/apt-groups

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.[64] Their efforts aim to discredit and hamper the operation of certain political or civil society actors. Instances have been noted in the Russian Federation, Belarus, Africa, South-East Asia, and across Latin America.[65] These actors can work independently, but also sometimes coordinate with clandestine services, criminal or independent groups to achieve their aims. 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. Examples of such tactics include the way Saudi Arabia utilized mobile phone spyware purchased from an Israeli company to monitor dissidents and political opponents.[66]

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.[67] Sometimes, however, it is suspected that criminal groups will work in concert with governments or foreign threat actors for either financial remuneration, political motivation, or due to pressure placed upon them. They have also been used by government actors to evade attribution. The willingness of cyber criminal groups to "sell" their expertise and resources has given rise to the term Cybercrime as a Service (CaaS). Criminal groups will, for example, "rent" their command and control of infected computers to direct requests that, through request overload, cause servers to crash. It should be noted that modern sophisticated criminal groups can use TTPs that sometimes approach or mirror the sophistication of state sponsored actors. This means that APT level sophistication can, potentially, be purchased and utilized by both state and non-state actors that do not themselves possess the resources for such attacks.[68]

---

[64] See Lindberg, S. (ed.). (2021, March). Autocratization Turns Viral: Democracy Report 2021. https://www.v-dem.net/files/25/DR%202021.pdf

[65] Robertson, J., M. Riley, and A. Willis. (2016, March 31). How to Hack an Election: Andres Sepulveda Rigged Elections Throughout Latin America for Almost a Decade. He Tells His Story for the First Time. Bloomberg. https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[66] Bergman, R. and M. Mazzetti. (2021, November 3). *Israeli Companies Aided Saudi Spying Despite Khashoggi Killing*. New York Times. https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

[67] Fung B. (2020, October 29). *Ransomware Hits Election Infrastructure in Georgia County.* CNN. https://edition.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html; and Organization for Security and Co-operation in Europe. (2019, August 21). *Republic of North Macedonia, Presidential Election, 21 April and 5 May 2019, ODIHR Election Observation Mission Final Report.* https://www.osce.org/files/f/documents/1/7/428369_1.pdf

[68] Vrabie, V. et al. (n.d.). *More Evidence of APT Hackers-for-Hire Used for Industrial Espionage.* Bitdefender. https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

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. While there are no specific examples of attacks by hacktivists or non-state political groups against election infrastructure at the time of this writing, there are many examples of hacktivist attacks against other governmental IT infrastructure in several countries, including within the United States.[69] This type of activity can be organized and domestically-based, and can be driven by transnational collaborators or individuals.[70] In addition, there are examples of foreign 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.[71]

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 into place controls for – insider threat mitigation. There are managerial, operational, and technical controls that are designed to help mitigate such threats. For example, sensitive IT processes should use "two-person" controls, whereby two people must sign-off and be involved to successfully complete the task. Another administrative (management) control would be the execution of background checks for EMB employees to help screen out candidates that are more likely to pose an insider threat. In terms of technical controls, automated alerting of suspicious activity such as copious printing outside normal business hours can be utilized to help identify possible exfiltration of data by insiders. These types of controls may not be achievable given the limited resources available to many EMBs.

Section VII: Emerging Cyber Threats in Elections

Historically, cyber threats have been characterized by two central trends: first, the speed at which malicious threats spread increases exponentially; and second, the scope of the systems affected by these threats widens exponentially.[72] Threats have increased in both sophistication and complexity—so defensive measures require further sophistication and complexity to match. This has given rise to a market for professional cybersecurity products, services, and tools. All indications are that cyber-based threats will only continue to evolve along these lines as election infrastructure moves toward further integration

---

[69] Bergal, Jenni. *'Hacktivists' Increasingly Target Local and State Government Computers.* PEW. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/01/10/hacktivists-increasingly-target-local-and-state-government-computers

[70] George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), 100249.

[71] Department of Justice Office of the United States Attorneys. (2018, May 29). *International Hacker-For-Hire Who Conspired With And Aided Russian FSB Officers Sentenced To Five Years In Prison*. https://www.justice.gov/usao-ndca/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-five

[72] This trend can be observed when assessing the speed at which various worms, viruses, and malware emerged and spread. In particular the period between 1989 and 2018 is detailed in Chaudhary, Tarun. (2019). *Coordinating across chaos: The practice of transnational internet security collaboration* (Doctoral dissertation, Georgia Institute of Technology). https://smartech.gatech.edu/handle/1853/61229

of digital technology. Election practitioners may only be beginning to grapple with how to integrate cybersecurity good practice and sophisticated defense across that evolving digital electoral infrastructure. Capacity within EMBs to strategically manage and respond to the challenge of cybersecurity will need to continue to be bolstered and resourced to meet that challenge.

Cyber threats will continue to evolve alongside the evolution of the information technology industry. For example, the trend toward hosted "cloud" services will put pressure on election managers to increasingly contract with third-party services to host and manage important infrastructure such as voter registration databases—putting important facets of the electoral process in the hands of commercial providers. Additionally, the desire for Internet-based voting is unlikely to abate. Promises of unassailably secure computing have yet to materialize despite decades of computer engineering devoted to the task; as systems of remote voting continue to be offered, it is likely threat actors will develop ways to exploit those systems.

Adversaries have identified cyberspace as an instrument of power and cyber attacks as a preferred method to achieve their aims across a spectrum of intentions, from causing general chaos to changing specific electoral outcomes. As such, election managers can expect a further evolution of the tactics and techniques used against election infrastructure, including more sophisticated methods of phishing and spear-phishing tailored to trick election personnel into disclosing sensitive details that allow threat actors to access sensitive systems. Supply chain attacks that target elections infrastructure vendors may become a growing concern. The use of cyber attacks to gain control of or access official sources of information, such as official websites, social media accounts, or other vectors that can be used to circulate misinformation and disinformation is also likely to continue. Adversarial innovation within the field should not be underestimated. The means for advanced tactics, techniques, and procedures have become ever more accessible through the emergence of CaaS, linking the intentions of politically motivated groups with the advanced capabilities of sophisticated criminals. This is likely to result in threats of increased sophistication from a wider variety of actors, including commercial and political interests that may not need vast financial resources to obtain such sophisticated capabilities, and pay-to-play organizations operating across and without regard to national borders or sovereign interest.

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

Section VIII. Glossary

Advanced persistent threat (APT): The level of sophistication associated with well-resourced malicious threat actors, often associated with foreign governments.

Attack surface: All possible entry points for unauthorized access into electronic information systems both physically and digitally.

Boundary delimitation: Drawing electoral district boundaries (or constituencies) and determining electoral precincts and polling locations and assigning voters accordingly. Typically takes place in the pre-electoral and post-electoral phases.

Cybersecurity: How electronically processed information can be secured against disruption, disablement, destruction or malicious control, thus protecting its integrity, availability and confidentiality.

Cyber hygiene: Term that is used to indicate the body of good practice that users of information systems should utilize in order to keep themselves and their data safe and secure.

Election dispute resolution (EDR): Complaints adjudication essential to the integrity and legitimacy of an election that increasingly use technology to facilitate disputes and resolutions.

Election management body (EMB): The core institution charged with administering a country's election process.

Electronic information: Any idea, concept, or data that is represented digitally and electronically processed. Electronic information can exist in three different states and can be stored, processed, or transmitted.

Information security dimensions: Confidentiality, integrity, and availability (often abbreviated as CIA).

Information security management: The tasks necessary to maintain the confidentiality, integrity, and availability of information as it is being stored, processed, and transmitted.

Tactics, techniques and procedures (TTPs): The universe of techniques and associated actions malicious actors employ to achieve their intentions

Threat actor: Person or group that engages in cyber-based attacks.

Vulnerabilities: Weaknesses in a system that an attacker may be able to successfully compromise. Computer vulnerabilities may exist for varied reasons.