I. INTRODUCTION

The process of planning for and administering democratic elections is one of the most complex, collaborative endeavors a country may undertake. The institutional context within which an election is managed and executed varies across many different democratic arrangements, but the core institution charged with administering a country's election process is commonly referred to as an election management body (EMB). The EMB has multiple responsibilities, including maintaining integrity throughout the planning process, carrying out elections, and finalizing results.[7] The continued integration and use of information technology within the broader process of electoral planning, management and execution is both necessary and desirable. As such, an EMB's mandate to protect the integrity of an election naturally extends to ensuring adequate cybersecurity for the information technology utilized across the spectrum of activities under its purview.

The term "cybersecurity" refers to the means through which electronically processed information can be secured against disruption, disablement, destruction or malicious control, thus protecting against the possibility of the information's integrity, availability or confidentiality becoming compromised.[8] The use of cyber-based attacks against public institutions – including those associated with election infrastructure – are a known and documented occurrence, and one that has occurred with increasing frequency, as noted in the next section.

OFTEN OBSERVED CYBER ATTACKS

DENIAL OF SERVICE	PHISHING	RANSOMWARE
Attackers make multiple requests that overload and cause a website or online resource to fail. Often attackers can purchase malicious services that utilize compromised computers connected to the internet under remote command and control that can be directed to make such requests. These networks are called "botnets" and perform a "distributed denial of service" attack.	Attackers use methods of deception to trick unsuspected users into clicking on malicious links that trigger the download of software that can compromise their system or deceive users into providing passwords that can then be utilized to compromise accounts.	Attackers compromise a network and encrypt data. The attackers may then contact a victim promising to send a decryption key in exchange for money.

[7] For a comprehensive overview of the various institutional arrangements associated with the management of democratic elections, see: Catt, Helena et al. (2014, September). *Electoral Management Design, Revised Edition.* International Institute for Democracy and Electoral Assistance. https://www.idea.int/sites/default/files/publications/electoral-management-design-2014.pdf

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

Elections all over the world have been targets of cyber attacks; in addition to the incidents mentioned below, there are examples across Europe, North America, Latin America,[9] Africa,[10] Asia,[11] and Oceania.[12] Citizens are generally aware that these attacks are likely, and many doubt – with good reason – that their respective countries are prepared to successfully counter them.[13] Recent elections in Kenya and the Democratic Republic of the Congo, for instance, have seen electronic results seemingly disappear into thin air — even without suspected external interference. Such self-inflicted cyber failures expose the need to enhance electoral technology security and reliability, improve user knowledge and training, introduce additional safeguards, and promote standard practices to reduce overall cybersecurity risks.

There are differing opinions as to whether election technology – especially electronic voting and results management systems – can be fully protected from cyber attacks. While some EMBs (such as Brazil's TSE[14]) and technology vendors, as well as successful electoral candidates, may insist that election technology can be fully protected, cybersecurity experts generally agree that there is no way to guarantee an absolute level of security against cyber threats and fully protect against all risks. While cybersecurity risks cannot be eliminated entirely, many can be mitigated with the application of security controls as part of a holistic cybersecurity strategy.

This report provides an overview of the more practical threats to elections and outlines the concept of cybersecurity as a risk management process that should be adopted by EMBs. The paper begins with an overview of technology adoption and cybersecurity threats in elections and a brief literature review of the existing body of work that informs electoral cybersecurity policy and practice.

Next, the paper discusses the primary actors posing cyber threats to election technology. It then applies the key cybersecurity concepts of risk management and security control mechanisms to the electoral process using a risk-based approach with a focus on mitigation strategies for election management bodies. The penultimate section considers the importance of multi-stakeholder coordination and outlines cyber risks for two additional stakeholder groups: political parties and civil society organizations.

The paper concludes with a discussion of areas where further analysis and guidance is needed to strengthen the cybersecurity postures of electoral management bodies.

[9] Marañon, A. (2021, May 28). *How Have Information Operations Affected the Integrity of Democratic Elections in Latin America?* Lawfare. https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democratic-elections-latin-america

[10] Allen, N. and N. van der Waag-Cowling. (2021, July 15). *How African States Can Tackle State-Backed Cyber Threats*. Brookings Institute. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

[11] 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

[12] Galloway, Anthony. (2020, October 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

[13] Poushter, J. and Fetterolf, J. (2019, January 9). *International Publics Brace for Cyberattacks on Elections*, Infrastructure, National Security. Pew Research Center. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[14] TeleSURtv.net. (2021, August 2). TSE de Brasil Respalda Sistema de Voto Electrónico. https://www.telesurtv.net/news/brasil-tse-respalda-sistema-voto-electronico-20210802-0026.html