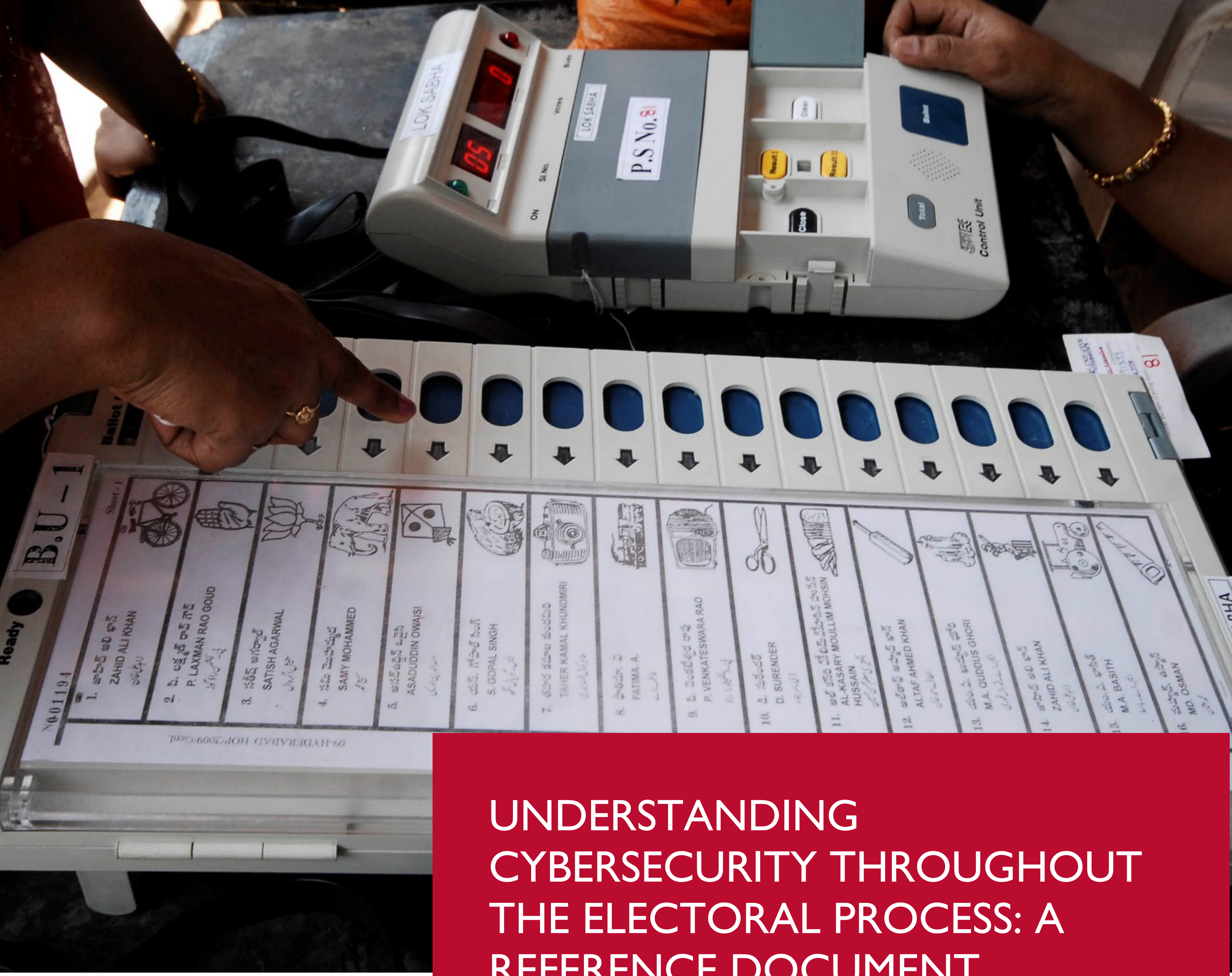

PHOTO © AP PHOTO/MAHESH KUMAR A. 2009

UNDERSTANDING CYBERSECURITY THROUGHOUT THE ELECTORAL PROCESS: A REFERENCE DOCUMENT

An Overview of Cyber Threats and Vulnerabilities in Elections

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

Acknowledgements

This reference document 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, Thomas Chanussot, and Dr. Manuel Wally were lead authors. The reference document benefited tremendously from contributions by Dr. Stephen Boyce, Dr. Beata Martin-Rozumiłowicz, Dr. Staffan Darnolf, Chelsea Dreher, Katherine Ellena, Brian Polk, Federico Roitman, Victoria Scott, Erica Shein, and Chad Vickery. The authors would also like to acknowledge Annie Styles for her immense help. 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

EXECUTIVE SUMMARY

Since electronic voting technology was first introduced, a variety of new technologies have been developed and integrated into elections around the world, affecting each step of the election process. In many cases, these technologies are efficient, reduce the risk of human error,[1] improve accessibility,[2] and can mitigate or prevent some types of election fraud.[3] As election management bodies (EMBs) have taken up new technologies – particularly around digitization of voter registries, transmission processes and aggregation of election results – multiple sources of policy, principle and practice in electoral cybersecurity have emerged to address the potential for disruptive cyber attacks.[4]

However, significant gaps remain in developing further guidance and regulation for EMBs, policymakers, and electoral stakeholders to ensure that electoral technology is secured from threats and trusted by the public. Failure to address electoral cybersecurity risks can pose a critical threat to electoral integrity. Malign actors may attempt to manipulate elections directly, undermine public confidence in elections, or erode the legitimacy of elected representatives and bodies by exploiting vulnerabilities in electronic information processing and cyberspace. Such loss in trust and concerns about legitimacy could impede development initiatives and undermine effective and accountable governance.

As the number of election technology applications grows, elections have begun to attract the attention of a wider spectrum of threat actors. Cyberspace, despite all the societal benefit and economic value it has helped create, is also an arena of strategic competition and criminal activity. The electronic information systems in use across electoral processes are therefore important elements of critical national infrastructure that can be attacked. There are well known examples of cyber attacks 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. Domestic actors have also emerged to threaten elections. They may be politically, financially, or ideologically motivated, and operate individually or collectively, but like their foreign counterparts they are finding ways to undermine trust in elections. The emergence of these domestic actors means that institutions charged with upholding the integrity of elections must also work to recognize and mitigate potential insider threats.

Election managers should look to trends identified within the wider field of cybersecurity analysis to understand the types of attacks that can potentially impact systems falling under their purview. While denial of service attacks that overload infrastructure and other relatively unsophisticated attacks are still occurring, recent analysis has highlighted how a commoditized market for sophisticated tools and methods

[1] Goldsmith, B. and H. Ruthrauff. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. National Democratic Institute and International Foundation for Electoral Systems. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies, pp. 21-22; and National Democratic Institute. (n.d.). The Rationale for E-voting in Brazil. https://www.ndi.org/e-voting-guide/examples/the-rationale-for-e-voting-in-brazil.

[2] Human Systems Integration Division, Electronic Systems Laboratory, Georgia Tech Research Institute, Georgia Institute of Technology. (2012, July). Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment. https://www.nist.gov/system/files/documents/2017/05/09/GTRI-Appendix-A-Accessibility-of-Voting-Systems.pdf

[3] Somanathan, M. (2019, April 5). India's Electoral Democracy: How EVMs Curb Electoral Fraud. Brookings Institute. https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/

[4] The attacks on Ukraine in 2014 and the United States in 2016 are particularly illuminating. See, for instance, Martin-Rozumilowicz, B. and T. Chanussot (2019). "Cybersecurity and Electoral Integrity: The Case of Ukraine, 2014-Present." In Krimmer, R. et al (Eds). Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019: 1-4 October 2019, Lochau/Bregenz, Austria: Proceedings. https://www.zora.uzh.ch/id/eprint/175950/

has lowered barriers and allowed lesser resourced actors to purchase greater malicious effect.[5] Threat actors often also use methods of deception to trick users into clicking on malicious links or disclosing sensitive information like passwords in a practice called "phishing." Often nation-state actors will utilize their intelligence resources to target individuals using content tailored or engineered specifically for that person in the practice of spear-phishing. Once sensitive information is obtained, it can often be leveraged to compromise systems and establish a foothold within a network. That foothold can then be utilized for any number of purposes. Criminal elements may, for example, deploy software that encrypts data in financial extortion schemes.[6] Nation-states or other sophisticated actors may use such a foothold to execute further penetration of a network and exfiltrate sensitive and confidential information they can leverage for intelligence purposes.

The range of stakeholders that are being targeted with cyber attacks – and are working to prevent and respond to them – is also expanding. For instance, EMBs have taken up a role in risk analysis, mitigation, and response to threats against their systems and equipment. Civil society organizations, political parties, and candidates have also been targeted by threat actors that are driven by distinct motives. Each stakeholder group must assess their own specific vulnerabilities and develop and take ownership of a cyber mitigation strategy.

Effective cyber threat detection and mitigation is characterized by a continuous and well-defined process of risk management that hews to industry best practices defined in several standard risk management frameworks. While governments and industry have widely adopted and typically follow these frameworks, adherence is often limited by resource availability, competing priorities and lack of cybersecurity advocacy.

The purpose of this report is to help USAID Democracy, Human Rights, and Governance (DRG) staff and other relevant U.S. Government personnel to better understand the nature of electoral cybersecurity risks and threats in the contexts in which they work. Drawing on the fields of both electoral management and cybersecurity risk management, it provides an entry-level overview of electoral cybersecurity threats, vulnerabilities, threat actors, and mitigation measures across key aspects of the electoral process. It also outlines good practices that EMBs can leverage to mitigate and address cyber threats.

The report is designed to be useful to individuals that may not have prior cybersecurity knowledge. It focuses on the risks and mitigation activities that EMBs and their partners might face during pre-election, election and post-election periods. By understanding the wide range of potential risks and threats they may face, EMBs will be better able to prioritize where to expend their resources and how to adapt existing risk management frameworks and cybersecurity good practices to their context.

It should be noted that 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, 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 to one involved stakeholder can have wide-reaching effects. Considering this reality, EMBs will need to work with other stakeholders (such as state offices that compile civil registries from which voters lists may be pulled, or authorities auditing voting machines)

[5] The Microsoft Digital Defense Report issued in October 2021 has recent trending data. See: Microsoft. (2021, October). Microsoft Digital Defense Report. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[6] The term ransomware is often used to describe this practice.

to establish mature cybersecurity postures to holistically recognize and manage the risks individually and collectively across the electoral process.

In particular, a review of recent trends indicates that EMBs and their partners may face particular challenges when it comes to protecting voter registration databases and results tabulation and transmission systems – which are attractive targets for cyber attacks to undermine stakeholder acceptance of electoral outcomes. 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 must be balanced with the risk that such resources may be compromised by malicious actors undermining election processes.

These risks can be further compounded by poor cyber hygiene among institutions and users involved in administering and maintaining election technology, along with *ad hoc* and piecemeal approaches to cybersecurity involving third parties, technology procurement and multi-stakeholder collaboration. Therefore, it is important that the concern of cybersecurity be addressed holistically throughout electoral infrastructure. EMBs need to educate users of electronic information systems in proper cyber-hygiene. Policies and processes that inculcate and support cybersecurity good practice need to be put in place, and EMBs will need to invest in executive oversight, advocacy, and management of cybersecurity through professionalized and dedicated workforce roles.