ace
project | projet | proyecto
The Electoral Knowledge Network

Newsletter
NOVEMBER 2018

YOUR PORTAL TO THE WORLD OF ELECTIONS

Cybersecurity in Elections: a HEAT Process for EMBs to protect themselves against cyber threats

Katherine Ellena and Goran Petrov, International Foundation for Electoral Systems (IFES)

The following is an excerpt from an IFES white paper. The full paper is available in the ACE "Cybersecurity in Elections" Encyclopaedia Topic and on IFES.org.

In June 2017, 100 election experts from across the United States penned an open letter to Congress noting that many jurisdictions were "inadequately prepared to deal with rising cybersecurity risks."[1] This concern is echoed globally, as increasing reliance on complex technology-based systems in electoral processes has left troves of sensitive information potentially vulnerable to adversaries.[2] Experiences in several recent elections around the world highlight threats to cybersecurity, as well as how the implementation of certain electronic data management technologies can impact post-election disputes.[3] However, many election management bodies (EMBs) lack the capacity, resources, or appropriate framework to test whether their data management systems are secure from these vulnerabilities, and to put measures in place well in advance of elections to protect data integrity.

Cybersecurity[4] should be considered and implemented at the inception phase of building or upgrading any technology-based election system, as a key component of digitizing specific elements of election administration. At the same time, international good practices around cybersecurity and open data require EMBs to act transparently and to ensure election results are verifiable and can ultimately be accepted by the electorate. Therefore, it is important to protect both cybersecurity and transparency in the electoral context – a challenge that is unique to EMBs.[5]

Beyond striking this balance, election administrators must focus on cybersecurity as an ongoing and ever-changing concern. As soon as cybersecurity good practices are developed, they may become outdated, because technology moves forward very quickly, as does the technical expertise of those who seek to find and exploit its vulnerabilities. While it is important to learn from experience, rapid technological innovation means that EMBs should endeavor to secure the next election, not focus on vulnerabilities in the last election. This means identifying potential future vulnerabilities, not only addressing issues that have been identified or exposed in the past.

It also means looking at cybersecurity holistically, as one type of vulnerability may be addressed in isolation while another is exploited instead. Or, different types of cybersecurity exposure may compound to produce a unique vulnerability that can result in significant problems, whether through malpractice (negligence or mistake) or fraud (deliberate exploitation).[6] While existing guidelines on cybersecurity, discussed in the literature review, provide sound guidance on mitigating technological exposure in elections (for example, by ensuring sound cyber hygiene practices and implementing two-factor authentication), they may not consider other types of exposure, such as restrictive laws, weak procedures or untrained staff, that can undercut cybersecurity frameworks and lead to breakdowns in the electoral process or in public trust of electoral outcomes.

Given all these considerations, how can EMBs secure systems from technical vulnerabilities that leave them exposed and may lead to post-election challenges, while at the same time protecting principles of open data and transparency?

Dear readers,

This year, the ACE Electoral Knowledge Network is celebrating **20 years** as the world's largest online source of electoral knowledge. To commemorate its many successes, ACE is launching a structural and visual revamp of its website and an Anniversary Timeline, highlighting key achievements since 1998.

Reaching more than 2.5 million visits per year, the ACE website provides more than 10,000 pages of knowledge resources in English, Arabic, French, and Spanish. ACE promotes credible and transparent electoral processes with an emphasis on trust, sustainability, and professionalism in the electoral process.

This edition of the ACE Newsletter highlights a new ACE Encyclopaedia Topic, Cybersecurity in Elections. The Newsletter further highlights:

- The latest questions and discussions on the Practitioners' Network
- New publications and resources from ACE partner organizations

Thank you for reading November's newsletter and for your involvement with ACE. We look forward to your contributions to the Network!

Sincerely,

The ACE Electoral Knowledge Network

In this paper, the International Foundation for Electoral Systems (IFES) outlines strategies for EMBs to strengthen their technology and procedures to resist vulnerabilities, by following what we have termed a Holistic Exposure and Adaptation Testing (HEAT) process. While no electoral process or technology is infallible, the HEAT process aims to secure automated or digitalized electoral processes – as far as possible – against unanticipated threats, illicit incursions, system failures, or unfounded legal challenges.

As the name suggests, the HEAT process focuses on the types of exposure an EMB may face when implementing different types of technology systems (technology, human, political, legal and procedural). Because the HEAT process seeks to provide a holistic approach to cybersecurity in elections, we have drawn lessons from international principles, election cybersecurity case studies, risk-mitigation methodologies and technology-related election court judgments. The proposed process is also guided by international best practices on data management and cybersecurity, as well as transparency, open data and privacy.

A thorough HEAT process, as described in this paper, has significant time and cost implications. However, without such a process in place, an EMB may experience an electoral crisis that far exceeds the time and resources invested in such a risk-mitigation process. It is important to note that a HEAT process is only suitable for the earlier part of the electoral cycle when there is significant time for the EMB to implement measures to mitigate identified deficiencies. While the HEAT process itself may be achievable in a short time period, it is often the case that cyber vulnerabilities cannot be addressed by "quick fixes," but require significant lead time to address properly. For example, if certain legal or procedural vulnerabilities are revealed, several months or more may be required to draft or pass amendments, or to adjust procedures and then train and publicize new procedures effectively. If a HEAT process is conducted and reveals vulnerabilities too close to an election to be able to rectify, this could then have an adverse effect on stakeholder confidence in the electoral process.[7] This is particularly true in environments with pre-existing low trust.

This paper outlines the existing literature on cybersecurity and data protection in elections, including international standards, good practice guidelines, cybersecurity frameworks, election observer guidelines, and jurisprudence. This literature is then applied to discuss the various types of exposure EMBs may face when implementing technology and seeking to protect data and data processing in elections. This application is important, as while much of the standard-setting is taking place in North America and Europe, in IFES' experience many developing democracies outside of these regions are also considering and using election technologies. Finally, the paper introduces the IFES HEAT process as a holistic tool for identifying and mitigating different types of cybersecurity exposure in elections.

[1] "Election Integrity Open Letter to Congress," National Election Defense Coalition.

[2] Two 11-year-olds altered election results in hacker convention's replica of U.S. voting system, Reuters, 2018.

[3] For example, electronic transmission of results at the polling station level or maintenance of national biometric voter registration databases, but also penetration of less high-profile databases such as personnel records for ad hoc staff, that could undermine the public's confidence in the EMB and its capacity to secure more sensitive databases.

[4] In this paper, IFES uses the terms "cybersecurity," "data security" and "data protection" inter-changeably, in line with ISO standards and academic literature. See, e.g., Basie Von Solms, Rossouw von Solms, Cyber security and information security – what goes where?, which offers that: "Cyber Security [is] part of Information Security, which specifically focuses on protecting the Confidentiality, Integrity and Availability (CIA) of digital information assets against any threats, which may arise from such assets being compromised via (using) the Internet."

[5] For example, other agencies such as defense, or institutions such as banks or insurance agencies, can focus primarily on cybersecurity without the same transparency concerns.

[6] IFES has defined these terms further in Assessing Electoral Fraud in New Democracies: Refining the Vocabulary.

[7] The Venice Commission's Good Practice in Electoral Matters includes a provision that the fundamental elements of the election legislation should not be fundamentally amended one year prior to a forthcoming elections

Practitioners' Network

Since April, **149 members** logged on to the Practitioners' Network and shared their experiences, knowledge and expertise through **25 contributions** to questions asked by their peers. Recent questions include: Plurality systems where a majority coalition can't override the election leader, Voter registration without link to national identification, Voters registering and voting outside their municipalities of residence, and "Head of list" election model.

Consolidated replies are published summaries of the discussions on the Practitioners' Network. The following page highlights some recently published consolidated replies, including: Observer accreditation by separate body, Voter registration authorities, Polling stations staffed by citizens, and EMB media strategies. Dozens of questions have been consolidated already, so be sure to look here for a full overview.

Join the Network!

- Are you an election practitioner with expertise and experience?
- Are you not yet a member of the ACE Practitioners' Network?

If so, submit an application to be a member of the Practitioners' Network now: www.aceproject.org/apply.

Recently Consolidated Questions

Voter registration authorities

I'm doing some background research on voter registration in non-Western contexts, and am interested in which bodies do voter registration in a country. For instance, in most U.S. states, citizen groups and NGOs can help citizens register and submit their applications to the election body. In contrast, in Kenya, the election commission is the only body legally allowed to register citizens. How does voter registration occur in the contexts you know? Is the electoral commission the only body that can legally register people, or can citizen groups/NGOs undertake registration and submit applications to the electoral commission? Anybody know of systematic info on this?

Observer accreditation by separate body

I am looking for examples of countries where observer accreditation is issued by a separate body, not by the EMB. I would appreciate specific examples along with relevant legal provisions.

Polling Stations Staffed by Citizens

In Mexico, polling stations are staffed by volunteers drawn from the electoral register. Presiding officers receive training from the electoral commission. This model is not only cost-effective, but contributes to citizen ownership of the process. In some areas, there has been a reduction in enthusiasm for volunteering as a polling official, and there even some who attend the training and then do not take up the function. What other countries have relevant experience in this field and could supply ideas or even information and training materials that could encourage participation as polling officials?

Additional information on this phenomenon can be found here.

ACE Encyclopaedia: The Latest Updates

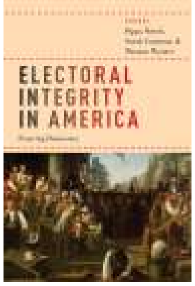
ACE has expanded its Encyclopaedia to include *Cybersecurity in Elections* (based on the paper featured in this newsletter) and, in the coming months, three more new topics: *Youth and Elections, Elections and Conflict,* and *Gender and Elections.*

If you would like to see a particular topic addressed in an ACE Focus On or translated into Spanish, French, or Arabic please send your suggestions to facilitators@aceproject.org.

Recent Publications by ACE Partners

When Are Elections Good Enough? Validating or Annulling Election Results (IFES)

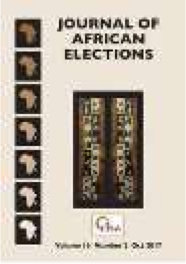
In this paper, IFES outlines various legal approaches to election annulments, explores different grounds for annulment, and outlines procedural considerations for courts and adjudicators when determining whether to annul an election result, drawing on international principles and global jurisprudence. It does not examine systemic issues, such as weak legal frameworks, or the distorting effect of private money in politics, but focuses instead on irregularities in the process that can call the legitimacy of an election into question. While annulments can happen in single polling places or in particular districts, this paper focuses on annulments of entire elections, especially at the national level, since they raise a distinct set of legal and practical problems and have particularly strong implications for the legitimacy of elections and democratic government more broadly.



America in Comparative Perspective (IFES) and Transparency (The Carter Center)

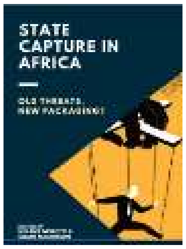
In chapters in the Oxford University Press publication, Electoral Integrity in America: Securing Democracy, IFES and The Carter Center analyze aspects of the U.S. electoral system. In this chapter, IFES evaluates key elements of the electoral process in the U.S. by applying the analytical framework of the IFES Electoral Integrity Assessment. The research seeks to answer the following question: How would technical assistance providers like IFES assess the integrity of the electoral process in the U.S., using the same parameters routinely used to judge developing democracies?

Nonpartisan election observation has become an almost universal global practice (Kelley 2012). By 2006, a total of 1,759 election events in 157 countries, or 80% of elections across the world, were observed by international organizations (Hyde 2011). Citizen observation activities were similarly widespread. However, the practice of observation in the United States is highly variable. In a chapter on transparency, The Carter Center presents research on questions regarding exactly who can observe what, when, and where, and the variations across the 50 states, particularly regarding nonpartisan observation, followed by an analysis of trends in policy and practice.



The Journal of African Elections Volume 17 Number 1 (EISA)

The Journal of African Elections (JAE) is an interdisciplinary biannual publication of research and writing in the human sciences, which seeks to promote a scholarly understanding of developments and change in Africa. This issue of the JAE includes articles on Angola's 2017 elections and the electoral processes in Angola; election violence in Kenya and South Africa; the role of election observers in Kenya's 2017 elections; local media observation in Mozambique elections; Internally Displaced Persons' voting rights in Nigeria's 2015 general elections; ethnicity and Nigeria's 2015 presidential election; youth participation in African elections; and Zanzibar's 2015 elections and the dissolution of the region's Government of National Unity.



State Capture in Africa: Old Threats, New Packaging? (EISA)

This edited volume explores the theory of state capture, especially in its contribution to democratic discourse in Africa. EISA seeks a firm understanding of state capture and provides recommendations on how such an understanding can add value to the analysis of governance in Africa. The volume is organized into three sections: Conceptualising State Capture, Capturing Democracy: The Hollowing Out of State Institutions, and Consequences of Capture and Lessons Learnt.

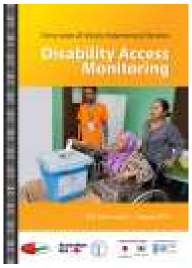
The JAE issue and this volume on state capture will be resources for anyone hoping to understand or analyze electoral processes throughout Africa.

International Consultative Workshop on Leveraging Electoral Training Facilities Globally (International IDEA)

In July 2017, International IDEA partnered with the India International Institute of Democracy and Election Management to host a two-day workshop for international electoral experts and professionals. This report focuses on the proceedings of that workshop. workshop was comprised of six sessions, and centered on institutional strengthening and professional development in elections. The report includes a "New Delhi Statement on Electoral Capacity Development," which focuses on guiding principles that recognize the importance of capacity development, enhancing electoral resources and professional competence for the conduct of elections. The Statement was adopted unanimously by the workshop participants, including representatives of EMBs from such countries as Nigeria, Georgia, and Nepal (among others). The report contains important tools and principles for other EMBs and electoral stakeholders.

Preventing Violence Against Women in Elections: A Programming Guide (UNDP) (EN, FR, ES)

This publication, jointly produced by UNDP and UN Women, brings to light the scourge of violence against women in elections.
It seeks to identify the specific components of violence against women in elections and presents options for policy and programming responses based on current good practices. It also provides examples of definitions and methods from all regions that may prompt ideas for actions. This guide is intended for those positioned to prevent and mitigate violence against women in elections as well as those providing programming support and other electoral stakeholders.



Disability Access Monitoring Report in the 2018 Parliamentary Elections of Timor-Leste (UNDP) (EN, Tetum)

UNDP partnered with IFES and Ra'es Hadomi Timor Oan (RHTO), a local CSO for persons with disabilities, to monitor the political campaign period and election day in Timor-Leste. This report is based on findings from that monitoring. It is a complete assessment of the access and facilities for people with disabilities in the political processes in Timor-Leste, including political campaigns, voter/civic education, processes, voter registration, and voting election-day. Several recommendations are provided in the report for giving full access to people with disabilities to the civic and electoral rights guaranteed under international law and the Constitution.