V. OTHER ELECTION STAKEHOLDERS

Elections are not simply procedural in nature. Rather, an understanding of electoral dynamics should account for interactions between an EMB, political parties, civil society, state apparatus and media, among other important stakeholders. While IT infrastructure is used for activities and tasks across the election process, an EMB will only be able to exercise direct agency and control over some subset of that IT infrastructure. In addition, because the secure and successful execution of an election involves information flowing among stakeholders, an obvious threat vector is the information flows themselves.

This fundamental need for coordination and information flow among disparate stakeholders can be characterized as happening across *seams*. Seams are defined as the gap across which information must traverse and coordination must occur between two or more distinctive functional units (for example an EMB, central government, civil registrar, and municipalities). Preventing the successful coordination and flow of information across these seams by targeting the confidentiality, integrity or availability of information is a likely tactic that an adversary may choose to utilize. Inter- and intra-agency seams are also important to note, since coordination barriers can arise not only through adversary targeting but also due to standard organizational challenges such as managerial gaps and stovepiping of information. Since much of that information and coordination may happen via electronic information technology, cybersecurity must be a central consideration for EMBs.[221]

The prior section of this report focused on technology usage across various components of the electoral process, and steps EMBs can take to identify and mitigate risks. This section briefly discusses the concept of multi-stakeholder coordination on cybersecurity in elections. It also highlights two important electoral stakeholder groups that may be targeted by threat actors: civil society organizations (CSOs) and political parties.

A. MULTI-STAKEHOLDER COORDINATION

There are various models of interagency collaboration during elections, including on transportation, security and public health, that are essential to the credible election administration. Although there are some good examples of multi-stakeholder coordination in the realm of election security – for example, the 2020 U.S. elections in which the Cybersecurity and Infrastructure Security Agency (CISA) played a critical supporting role to local and state-level election administrators and the coordination in the 2019 Ukrainian elections between the Ukrainian security services and the Central Election Commission (CEC) – the field is under-studied and would benefit from more research. Ensuring effective cybersecurity in elections in particular may necessarily transcend the traditional mandates and capacities of institutions – particularly EMBs. Effective cybersecurity may require resources that an EMB is unlikely to be able to gather on its own, as well as a comprehensive threat awareness and detection/deterrence capability that requires information and data exchange and response from multiple agencies.

There are multiple models of multi-stakeholder collaboration (formal or informal). Some are purely inter-agency, involving different government departments and independent institutions such as the EMB. Others include state and non-state agencies (including private sector vendors, social media providers, media and academia). Some coordination efforts are organized into thematic task forces (for example, a disinformation task force, or an online voting task force, while others focus on specific parts of the

[221] The concept of seams is discussed in detail within and adapted from Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). *Patchwork of Confusion: The Cybersecurity Coordination Problem*. Journal of Cybersecurity, 4(1).

electoral process (for example, collaboration on training of poll workers ahead of elections, or collaboration via a "war room" to track threats on Election Day itself). The specific political and institutional context – as well as the specific resource needs and vulnerabilities – will dictate the best mode of collaboration between multiple agencies and stakeholders on issues surrounding cybersecurity.[222]

A critical consideration around multi-stakeholder coordination is the fact that the independence and the perception of independence of the EMB must be safeguarded. Hence, any interagency collaboration should be publicly explained in a transparent and clearly defined manner. Each party that is engaged during cybersecurity activities must agree on the terms and context of that engagement. This is usually done through defined rules of engagement. Rules of engagement provide a defined framework for how different actors and institutions will respond to identified cyber-threats. The intervention (or non-intervention) of government agencies during an ongoing cyber-attack can be, in some countries and in some contexts, politically charged. Accordingly, clear rules should be determined in advance and communicated to all election stakeholders. These rules should be sufficiently detailed so there is no ambiguity with regards to roles and responsibilities, while giving sufficient leeway for actors to efficiently respond to an incident in a coordinated way. A balance must also be struck between transparency of any cybersecurity response, and the security of the protective measures themselves, to limit opportunities for bad actors to capitalize on freely available information about election cybersecurity platforms and processes.

Successful interagency collaboration and coordinated incident response will depend on whether there is a common understanding of roles, responsibilities, and communication channels. Technical simulations or strategic tabletop exercises can help organizations by rehearsing these roles and testing these channels, while also allowing those organizations to build and refine incident response mechanisms and procedures outside of (and well before) in the high stress environment of an electoral event.

B. CIVIL SOCIETY ORGANIZATIONS

Civil society plays a vital role in promoting government accountability, and civil society organizations (CSOs) that are focused on elections can help inform the public about a range of electoral issues – including the security of voting data and processes. Moreover, CSOs that understand election technology and its associated benefits and risks can provide an external, independent perspective on key technology or cybersecurity decisions made by the government, legislature, or election officials and offer informed, independent advice, ideally helping to strengthen EMBs and elections more generally. This advice can help officials consider the end users of election technology and information needs that may need to be built into poll worker training or voter education.

In many countries, national and local CSOs play a key role in oversight of the electoral process, and election-day observation. Citizen (domestic) election monitoring efforts can help encourage adherence to election procedures, improving public confidence in the integrity of the election (when warranted). However, given the sensitivity of election monitoring in some countries, and the potential political impact of such reporting, there are some cybersecurity vulnerabilities for CSO observers. This can include the insecurity of databases containing observer information (such as names, locations, email addresses, phone

[222] See, for example International IDEA's Models of Interagency Collaboration: van der Staak, S. and P. Wolf. (2019). *Cybersecurity in Elections: Models of Interagency Collaboration.* International IDEA. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

numbers). Databases containing observers' PII[223] are vulnerable to breach of confidentiality. The integrity of observation data and draft observation reports could also be undermined if no safeguards are in place. For example, when default accounts and credentials (often put in place by software/hardware providers for initial configuration) that have not been further secured remain in place and are accessed by users, data can be compromised and used by adversaries.[224] Finally, the transmission of observer reports and communications via insecure methods of communication can prove vulnerable to interception, for example if such reports are transmitted via common, unencrypted email.

These vulnerabilities, if exploited, can reduce public trust in the integrity of a given CSO, and in the broader election process. It can also leave CSO staff and observers vulnerable, particularly in repressive or closing political environments where CSOs may be under broader attack or scrutiny. As such, it is important for CSOs to maintain strong control of their internal communication and to protect the secure nature of their privileged relationships with key government partners. Hostile actors can gain access to such communication, often through phishing or spear-phishing attacks on CSO staff,[225] brute force attacks (where hackers attempt to guess a password to gain entry to a CSO's internal communication systems),[226] or communication interception through the exploitation of insecure WIFI networks or other unsecure channels.

To mitigate these risks, CSOs should implement organization-wide cybersecurity measures, starting with robust cyber hygiene training that can help reduce the likelihood and impact of common attacks. CSOs should also prioritize using full disk encryption on hardware and physical security tokens, especially if working in politically hostile environments. Finally, CSOs should seek to reduce or eliminate information and data exchange via insecure means of communication, such as SMS or public Wi-Fi networks, and instead use end-to-end encrypted messaging platforms.[227]

C. POLITICAL PARTIES

Regular internal communication and electronic information exchange are integral parts of the day-to-day operations of a political party. These communications can span a wide range of topics, some politically sensitive – such as draft policy positions, opposition research and campaign strategies – and some involving personal information – such as personal vetting documents and correspondence with donors. The systems used for these communications can vary widely and include email accounts, cell phones, landlines, SMS text messages, third-party messaging applications, web-based platforms, computers, databases, smartphones and mass messaging applications.

Additionally, in many countries political parties have tens of thousands of members, and sometimes affiliate groups associated with the party. Political parties need to store information for all the members associated

---

[223] McCallister, E., T. Grance and K Scarfone. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information*. National Institute of Standards and Technology. Vol. 800, No. 122. https://csrc.nist.gov/publications/detail/sp/800-122/final

[224] Cybersecurity & Infrastructure Security Agency. (2013, June 24). *Alert (TA13-175A) Risk of Default Passwords on the Internet.* https://us-cert.cisa.gov/ncas/alerts/TA13-175A

[225] Cybersecurity and Infrastructure Security Agency. (2019). Phishing. https://www.cisa.gov/sites/default/files/publications/NCSAM_Phishing_2020.pdf

[226] Esheridan. (n.d.). *Blocking Brute Force Attacks.* OWASP. https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

[227] Ermoshina, K., F. Musiani, and H. Halpin. (2016, September). "End-to-End Encrypted Messaging Protocols: An Overview." In International Conference on Internet Science. Springer, Cham. pp. 244-254.

with their party, including PII and donor contributions and expenditures. They typically store this information in a database or customer relationship management (CRM) solution, both of which could be susceptible to cyber attacks. Accordingly, parties should secure these information storage solutions using encryption and industry standard protections.

Given the sensitivity of party communication and information, and the potential for data misuse, political parties can be particularly vulnerable targets for cyber attack. In addition to undermining their electoral efforts, researchers have also noted that targeting the private data of candidates may have a chilling effect and deter candidates from participating in elections altogether.[228] In 2016, operatives hacked the server of the Democratic National Committee (DNC) in the United States. Twelve Russian military officers were charged with breaking into the Democratic Party's computers, stealing compromising information and selectively releasing it to undermine specific candidates.[229] Members of the German *Bundestag* were targeted with phishing attacks on their email accounts in 2015, and again in 2021 in the run-up to parliamentary election, in what was suspected collusion between right-wing domestic groups and the Russian GRU.[230] The French *En Marche* political party's handling of a 2017 breach in their communications provides an example of a sophisticated and effective response: the party's IT team identified the breach in its early stage and applied a strategy of *cyber-blurring*, injecting fake information and creating fake accounts among legitimate, though compromised, accounts. This action slowed the efforts of the adversaries without alerting them to the fact that they had been detected, ultimately reducing the value of the data that was exfiltrated.

Political parties must also manage a number of additional risks. These include the risk that insufficiently trained staff and volunteers are not able to recognize and avoid cybersecurity threats like those posed by phishing and social engineering attacks. There is also the risk that communication via insecure computers and smartphones will be intercepted or compromised. Insiders with malicious intent can pose a threat as well.[231]

To combat these threats and mitigate risks, political parties should regularly conduct cyber hygiene training, ensure that party email accounts have spam and phishing protection, enable full disk encryption on all hardware (to include the use of physical security tokens), use end-to-end encrypted communication platforms, and configure data loss prevention software for all sensitive documents and data. Beyond stop-gap measures to improve their security postures, political parties should consider hiring dedicated cybersecurity staff at least during campaigning periods and should strive to implement holistic cybersecurity risk management programs. Facing sophisticated and persistent adversaries will require political parties to be agile and to understand both risk mitigation and incident response – knowledge they are unlikely to acquire without the aid of external experts.

---

[228] Tenove et al. (2018)

[229] Whitaker, B. (2020, August 23). *How Russian intelligence officers interfered in the 2016 election.* CBS News. https://www.cbsnews.com/news/russian-hackers-2016-election-democratic-congressional-campaign-committee-60-minutes-2020-08-23/

[230] Zeit Online. (2021, March 26). *Russische Hacker Attackieren Offenbar Bundestag.* https://www.zeit.de/politik/deutschland/2021-03/cyberangriff-russland-hacker-bundestag-ghostwriter-geheimdienst-gru-cyberwar

[231] Hunker, J., & Probst, C. W. (2011). *Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques.* J. Wirel. Mob. Networks Ubiquitous Computer. Dependable Appl., 2(1), 4-27.

Finally, both political parties and CSOs (as well as other stakeholders) should take note of the recent Pegasus leak, which revealed widespread use of cyber-surveillance tools by governments.[232] The information that has emerged from the leak shows that governments can procure and use sophisticated cyber methods to monitor the activities of their political opposition, as well as journalists and civil society members that operate in their countries. High profile political targets should call upon specialized agencies or vendors to secure their devices; otherwise, as a protective measure, they should assume their devices are compromised and engage in communications accordingly.

[232] Pegasus is spyware sold by the Israeli company NSO Group which allows surveillance of mobile communications. It is marketed as a tool for monitoring criminal activity, but has been used by governments to monitor and target CSOs, journalists, activists and members of political opposition parties deemed controversial or threatening to ruling governments. The Pegasus Project (led by Amnesty International, Forbidden Stories and the Organized Crime and Corruption Reporting Project) aims to expose how Pegasus is being exploited. See Organized Crime and Corruption Reporting Project (n.d.). The Pegasus Project. https://www.occrp.org/en/the-pegasus-project/