III. APPLYING A RISK-BASED LENS TO ELECTION CYBERSECURITY

As information technology environments have developed and evolved, becoming more complex over time, the field of cybersecurity was born out of necessity. As the threats that take advantage of this complex environment have become more sophisticated, the cybersecurity field has become professionalized over time, evolving past the stage of simple checklists that indicate requirements for IT generalists to implement; modern frameworks instead characterize cyber threat detection and mitigation as a continuous process of risk management with industry standard practices to be performed by specialists.

A. RISK MANAGEMENT FRAMEWORKS

Risk management is a discipline in and of itself and there are several standard risk management frameworks. The most commonly used are: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, which is specific to information technology contexts;[114] the International Organization for Standardization (ISO) 31000 series, which is a generic risk management framework and

[108] Ibid.

[109] Park, Specter, Narula, and Rivest, *Going from Bad to Worse*.

[110] Ibid.

[111] Specter, M. A., Koppel, J., & Weitzner, D. (2020). *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections*. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 1535-1553).

[112] Ibid.

[113] Gaudry, P., and A. Golovnev. (2020, February). *Breaking the Encryption Scheme of the Moscow Internet Voting System*. In International Conference on Financial Cryptography and Data Security (pp. 32-49). Springer, Cham.

[114] NIST SP 800-37 is specific to the information technology concepts. It is available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

can be applied in conjunction with ISO 27001 IT controls.[115] The European Union Agency for Cybersecurity (ENISA) Risk Management/Risk Assessment (RM/RA) framework is also a comprehensive source of risk management standards and security controls.[116] Each of these frameworks – and the associated sets of security and privacy controls (discussed below) – have been designed based on specific national requirements, policies and laws. For example, the NIST framework was designed based on the U.S. context, while the ENISA framework is responsive to the European context. Governments and industry have widely adopted and typically follow them in the absence of a national framework. However, adherence to and implementation of these frameworks is often limited by strained resources, competing priorities and lack of cybersecurity advocacy.

The purpose of this section is not to endorse any specific framework and associated controls, but rather to introduce risk management and security control mechanisms generally, and to discuss cybersecurity as applied across the election cycle. [117]

Risk Management as a Continuous Cycle

The risk management process, as applied to electronically processed information, requires cybersecurity specialists to:

1. identify information and technology assets;
2. categorize both in terms of the impact of a potential loss or compromise;
3. assign and apply security and privacy controls based on prior categorization;
4. continuously evaluate the efficacy of those controls; and
5. feed information back into the process to continuously and proactively improve the controls.

B. CONTROLS, TRANSFERRANCE AND ACCEPTANCE

While the premise is simple, operationalizing cybersecurity risk management in electoral cycles is not a trivial task. Security controls are descriptions of discrete actions that can be taken to help mitigate risks.[118]

[115] The ISO 31000 framework is a general risk management framework that can be applied in various contexts, not just IT. https://www.iso.org/iso-31000-risk-management.html; the ISO 27001 standard establishes information technology security controls to be applied within the larger risk management framework.
[116] European Union Agency for Cybersecurity. (n.d.). *ENISA RM/RA Framework*. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework
[117] This is a simplification for understanding and brevity of the process described in depth within NIST, ISO, ENISA and other risk management frameworks.
[118] NIST SP 800-53 Rev. 5 defines a core set of security and privacy controls that operationalize the framework elucidated in 800-37. U.S. Department of Commerce and National Institute of Standards and Technology. (2020, September). *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Different frameworks separate controls into various aggregations, but the following three categories are useful for this discussion:[119] management controls, operational controls, and technical controls.

COMMON CATEGORIES OF SECURITY CONTROLS

MANAGEMENT CONTROLS	OPERATIONAL CONTROLS	TECHNICAL CONTROLS
Management controls are safeguards that focus on identifying and mitigating risks to information security through the use of assessments, audits, and planning.[120]	Operational controls are safety and security measures that are implemented and executed by human beings as they use, interact, and manage electronic information systems. [121]	Technical controls are safeguards that are generally embedded within hardware, software and firmware to protect information. A common example is encryption.[122]

Management controls use planning and assessment methods to help control risk (e.g., programmatic guidelines and policies, assessments to understand efficacy of budget planning and other enterprise-wide policies and protections that are scoped and executed administratively). *Operational controls* address the policies and protections that contribute to the secure operation of information systems throughout the lifecycle of a system, and are implemented through people executing processes (e.g., mandating specific change management steps, contingency planning or awareness training). *Technical controls* are implemented through the use of technology (e.g., encryption of data at rest and during transmission, automated monitoring and alarming and the use of verifiable security tokens to prove identity).

The controls themselves are put into practice at - and pertain to - various levels, ranging from the abstract cybersecurity program level (managing and implementing organized cybersecurity across an enterprise) down to physical hardware and software controls that implement specific security mechanisms. In addition to the program level, other commonly used categories include the site level (e.g., within a facility or across a location), the network level, the environment level (i.e., aggregated systems that are part of a cohesive whole, such as the server environment or wireless access environment), and the host level (referring to a single computer system).

Controls, however, are not the only way to manage cybersecurity risk. Risk can also be transferred via mechanisms such as insurance, through contractual relationships, or between agencies or departments due to division of responsibilities. Within the election space, such risk transference mechanisms may not be easily utilized nor appropriate, depending on, among other things, the type of EMB institutional arrangement or national policies and legal frameworks. In cases where risk cannot be mitigated or transferred, it can be accepted to facilitate operations. If risk is deemed too great, the information system or technology can be rejected for use. If the decision is made to adopt the system or technology despite the risks, the system is considered authorized. In this case, it should be managed throughout its lifecycle,

[119] 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/

[120] Ibid., p. 9.

from procurement through disposal, within the defined risk management framework.[121] Controls also involve defining the mechanisms of response during cybersecurity incidents.[122] Planning for response and post-event resiliency is an integral part of managing cybersecurity risk.

On the whole, a well-defined cybersecurity risk management process puts in place a holistic mechanism to understand and manage the risk of operating information systems and electronic networks. Executing the process identifies risks that are either mitigated, transferred (in contexts where appropriate and if circumstances allow), or in some cases accepted. This accepted risk is then identified and tracked within a risk register. Risk registers are continuously updated as new risks are identified and others retired (which takes place when controls are developed and applied to mitigate known risks, or when risks are eliminated).[123]

C. ADOPTING AND ADAPTING RISK MANAGMENT STRATEGIES

Effective cybersecurity requires buy-in at the executive level, as well as implementation throughout all levels of an organization. In the context of elections, EMB leadership is often risk-averse when it comes to modern technologies. The prospect of adopting new technologies to replace or complement traditional mechanisms used in electoral processes is daunting to many EMBs, as they consistently face limited time, resources, and capacity. It is therefore unsurprising to note that EMBs have, generally, been slow to adopt comprehensive cybersecurity risk management programs using dedicated resources and professional roles.

As noted in the IFES paper "Raising Trust in Electoral Technology," "Not only do many [EMBs] struggle to establish appropriate procedures and training for the new technologies, they also unfortunately neglect to maintain their traditional mechanisms. The compounding nature of these two factors create immense risks for their election."[124] In other cases, EMB executives may have unrealistic expectations that new technologies will have a positive impact on electoral processes. Successfully introducing, managing and cost-effectively maintaining technologies can be highly complex and challenging. This is especially the case in countries where the election authorities have

> "One fundamental problem is that the discussion, decision and implementation of new technology sucks out too much oxygen of many EMBs who have limited time and resources. Not only do many struggle to establish appropriate procedures and training for the new technologies, they also unfortunately neglect to maintain their traditional mechanisms. The compounding nature of these two factors create immense risks for their election."
>
> **- Peter Erben, "Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches," p. 3, 2017.**

[121] 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.
[122] The particulars of which are also not defined nor developed within the present discussion.
[123] 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.
[124] Erben, Peter. (2017). *Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches*. International Foundation for Electoral Systems. https://www.ifes.org/sites/default/files/ifes_erben_raising_trust_in_electoral_technology_innovation_aided_by_traditional_approaches_d8_sep_2017.pdf

limited previous experiences in holistically reviewing the risks and rewards of the investment. Too often, technology has been introduced to overcome what is inherently a political issue, lack of proper planning within the EMB, or to overcome the Commission's insufficient quality control capabilities of its field operations.

As such, the threat environment is likely to outpace an EMB's technology adoption; simultaneously, user practices consistently evolve ahead of new policy adoption, creating areas of unaccounted risk. Given this, the threat environment should drive EMB management to seek and advocate for necessary increases in resources, training and procurement, in addition to encouraging them to install policies to reduce cybersecurity risks. In modern organizations, cyber risk management is a matter of strategic planning and a key responsibility of executives, not simply a matter for IT departments functioning in vacuums to address.

Globally, there have been only limited efforts taken by EMBs to systematically mitigate cyber-related risks. There is, however, an increasingly explicit understanding that actors interacting with a system bear responsibility for, and must be involved in, its cybersecurity. Previously, election administrators understood their role to be that of a civil servant administering a bureaucratic process from behind the curtain; however, the last decade has made them front-line workers and first responders addressing critical situations that impact national security. To keep up with the evolution of the threat environment and evolve their cybersecurity postures accordingly, EMBs and other institutions must first assess and understand their current cybersecurity capacity strengths and gaps.

The concept of *maturity* is widely used in the cybersecurity community to refer to the ability and capacity of a cybersecurity program to help an organization to identify, detect, deter, and respond to threats unique to their organization or field. Maturity models help organizations locate their baseline cybersecurity activity on a scale and identify their desired future state. Maturity indicators can not only help to understand the programmatic and managerial characteristics of an organization's cybersecurity position, but they are also necessary to evaluate the cybersecurity workforce. The U.S., for example, has developed the National Initiative for Cybersecurity Education (NICE) Framework. The NICE framework defines seven high-level categories of common cybersecurity functions and 52 separate work roles. Each work role has defined skills and knowledge associated with it, which help guide measures of

Illustrative Maturity Model [127]

Level 3: Adaptable and proactive cybersecurity posture

Level 2: Cybersecurity practices are documented and there is institutionalized support and resources for those documented processes. The organization may still take a reactive approach to cybersecurity.

Level 1: Some practices and capabilities are in place, albeit ad hoc in nature

Level 0: Absence of cybersecurity activities and practices

[125] For a broad overview of the concept of maturity models, along with a U.S.-based example, see the Cybersecurity Capability Maturity Model (C2M2) available here: Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy. (n.d.). *Cybersecurity Capability Maturity Model (C2M2)*. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

maturity to determine the baseline skillset required of persons filling those roles.[126]

There are obvious challenges preventing EMBs from embracing and implementing comprehensive risk management-based cybersecurity programs across the activities that fall under their responsibility. These include the unique EMB institutional arrangements in various countries across various contexts, limited resources and competing priorities, immature national and local cybersecurity mechanisms, a lack of cybersecurity education, and a range of operational and technical impediments. However, introducing the risk-management approach to defining, understanding, and discussing these challenges can help clarify steps EMBs can take toward strengthening their cybersecurity postures. There are several countries that already have policies in place requiring EMBs to implement the risk management approach for cybersecurity via the frameworks referenced above, however uptake is far from institutionalized and substantial progress remains to be made.[127]

The following sub-section will present a short discussion of cyber adversaries. It is followed by content on illustrative threats, vulnerabilities, and mitigation across various components of the electoral process. It is helpful to view the mitigations discussed below through the lens of the three previously introduced, basic control types: management, operational and technical. These control types can be integrated into mature risk management mechanisms tailored to the electoral context. Given the dynamic nature of cybersecurity, and the multiplicity of contexts EMBs around the world face, this discussion is not, and cannot be, comprehensive. Instead, this discussion will first highlight how the idea of risk management can be introduced to clarify the challenge of cybersecurity for EMBs and will then identify areas where further guidance is needed.

D. THREAT ACTORS

A key part of assessing cybersecurity risk means understanding, as fully as possible, the threat actors. This discussion will define categories of actors and speak briefly about the types of tactics, techniques, and procedures employed by such adversaries. Tactics, Techniques, and Procedures (TTPs), as a concept, are broadly used by the security community (both physical and cyber) 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 certain threat actors from others. In addition, risk management frameworks use comprehensive understanding of TTPs to engineer controls to provide holistic defense mechanisms. The discussion of cybersecurity TTPs can easily extend into granular technical dimensions; as such, this report will only provide an introduction of how various threat actors employ and favor specific methods, tools, and actions.[128]

Disinformation as a tactic to undermine public confidence has emerged as a key component within the election space, especially since 2016. Populist politicians in developing countries have long sought to blame election technology vulnerabilities for their electoral defeats, but this trend has now also taken hold in major consolidated democracies — both in the pre- and the post-electoral context. The fallout of such

[126] Available here: National Initiative for Cybersecurity Careers and Studies. (n.d.). *Workforce Framework for Cybersecurity (NICE Framework)*. https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[127] One such example of the integrating ISO 27001 standards can be found in the Republic of Moldova: Republic of Moldova (2017). *Central Electoral Commission: 20 Years of Permanent Activity*. https://a.cec.md/storage/old_site_files/files/files/20%20ani%20CEC/Cartea_Cec_20_ani_eng_compressed.pdf
[128] 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

demagoguery has led to multi-million-dollar tort suits by the election technology industry.[129] Worse, it has eroded public confidence in elections among large segments of the electorate.[130] While it remains true that election technology cannot be completely protected against cyber threats, the lines between hypothetical residual vulnerabilities and successful cyber attacks have blurred in the public consciousness.

Within each broad category there are entities that are seeking to disrupt and undermine public confidence in elections, or to prevent a periodically scheduled election from taking place, either to extend their own mandate, or to thwart the overall democratic process. Over the last decade, the array of threat actors has widened considerably.

The categories below are introduced to support basic understanding of the different types of actors that may pose a threat to elections, but they do not operate in silos. Foreign state actors may cooperate with domestic political groups or criminal groups for example, where their objectives align.

1. FOREIGN STATE ACTORS AND ADVANCED PERSISTENT THREATS

Malicious actors associated with or directly tied to foreign governments constitute a grave threat within the election security space. 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.[131] Specific motivations and objectives may vary from target to target and among the purveyors of such attacks. 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.[132] Malicious threat actors associated with foreign governments are generally well-resourced and utilize sophisticated techniques. The level of sophistication is described by the term "Advanced Persistent Threat" or APT, and there are different industry and government designations for important 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 Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center.[133] APT 29, also known within the industry as "Cozy Bear," is attached to the Russian Foreign Intelligence Service (SVR).[134] Both groups have been responsible for some of the highest visibility and

[129] 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

[130] 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/

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

[132] 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

[133] 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/

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

effective cyber operations against elections entities over the past several years.[135] Identifying operations carried out by APT 28 and APT 29 relies, in part, on assessing the TTPs utilized. 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. APT 28 and APT 29 have access to a large supply of zero-days that highlight their relationship to government resources; such exploits would require sustained research and experimentation to identify.[136]

In addition, these well-resourced groups are able to 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). Spear-phishing is a targeted variant of the tactic of "phishing" where an adversary tries to harvest credentials and passwords from unsuspecting users by tricking them. Usually this involves sending an email with a malicious attachment or crafting webpages designed to capture user credentials and relies on unsuspecting victims believing the web page/email is legitimate. APT level threats use sophisticated intelligence and reconnaissance techniques to craft content presented to the target in a way that makes it hard for victims, even persons that have had training, to distinguish the 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.[137]

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.[138] Their efforts are often targeted at undermining the credibility of certain political or civil society actors, especially where there is a possibility of them making inroads through electoral processes. Instances have been noted in places like the Russian Federation, Belarus, Africa, South-East Asia, and all across Latin America.[139] 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.[140]

[135] 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
[136] Ibid.
[137] Mandiant. (n.d.). *Advanced Persistent Threat Groups.* https://www.mandiant.com/resources/apt-groups
[138] See Lindberg, S. (ed.). (2021, March). Autocratization Turns Viral: Democracy Report 2021. https://www.v-dem.net/files/25/DR%202021.pdf
[139] 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/
[140] 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

3. CRIMINAL GROUPS

Criminal groups are often involved in cyber crime for financial gain (for instance, ransomware attacks against state institutions). There is little official record of EMBs paying a ransom to recover its data, and it seems that in most cases, election administrations were collateral damage from larger attacks on government infrastructure.[141] 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. This type of attack is called a distributed denial of service or (DDoS). It should be noted that modern sophisticated criminal groups can utilize 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.[142]

4. NON-STATE POLITICAL GROUPS AND HACKTIVISTS

Criminal activity attributed to non-state political groups (including political parties and candidates themselves engaging in malicious activity) and activist individuals can also potentially target election-related infrastructure and other parties, candidates, or related (e.g., fundraising, and political) organizations. Hacktivist 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 and within the United States.[143] This activity can be organized and domestically-based, and can be driven by transnational collaborators or individuals.[144] 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.[145]

5. INSIDER THREATS

Individual or collective threat actors might also operate from within EMBs. Understanding the motivations of insiders that decide to act against the interests of their employer is difficult. However, a key component of any comprehensive cybersecurity program is to assess the threat of – and put into place controls for –

[141] 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

[142] 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

[143] 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

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

[145] 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

insider threat mitigation. Insider threat within the context of EMB operations is still poorly understood and thereby even more difficult to detect and/or address. There are, however, managerial, operational, and technical controls that are designed to help mitigate such threats. For example, sensitive IT processes should utilize "two-person" control whereby two people have to 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 resources available to certain EMBs.

IV. EMB RISK MITIGATION ACROSS THE ELECTORAL PROCESS

Election processes are complex and multifaceted, and vary across democratic systems and contexts. The following subsections highlight the technologies and processes involved with various important tasks in elections, with an emphasis on cybersecurity risks, threats, and mitigation strategies. The controls discussed throughout this sub-section are considered good practices that can be replicated and utilized across an EMB's information technology infrastructure and developed further as EMBs mature their cybersecurity risk management practices.

SELECT STRATEGIES FOR EMBS TO MITIGATE AND ADDRESS CYBER THREATS IN ELECTIONS

All functional teams in an EMB can and should contribute to a continuous and holistic culture of cybersecurity both within the institution and among voters: legal, communications, media/public affairs, operations, procurement, as well as information technology.

An EMB's government, peer organizations, and vendors are critical partners in reinforcing a local and international culture of cybersecurity.

Read further for more information but in general, EMBs should:

- Use the concept of least privilege to maintain control of sensitive information and systems, and use clear criteria for when access is allowed and when it should be revoked.
- Enable encryption, test and standardize security settings, and harden/limit functionality of hardware and software, especially remote/internet access.
- Design full chains of custody with regular integrity checks for all electronic and physical assets, from initial procurement to the end of life and disposal for the asset as required by law and in accordance with good practice.
- Practice, test, and simulate a variety of cybersecurity events and attacks, ideally with partners or independent parties. This produces valuable data for an EMB's procurement, security, response, and recovery plans—which, to emphasize, should involve all functional teams.
- Recognize the benefit of improved cyber hygiene and regular training at every level (high-profile political targets, candidates; judges, lawyers, clerks; election staff to EMB leadership and voters/general public).
- Maintain transparent, accessible systems with paper backups for results, audits, decisions, complaints and their responses. Paper backups are also useful tools in certain, but not all operational contingency plans.