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.

VI. CONCLUSIONS

The analysis in this report illustrates the way electronic information systems are heavily utilized across the electoral process. In cybersecurity terms, that infrastructure represents an expansive "attack surface" that can be threatened and exploited by foreign or domestic adversaries who intend to disrupt the electoral process.

While some established democracies have rolled back their use of technology for specific aspects of election administration, overall, the further digitization of the electoral process will likely only increase. In fact, the COVID-19 pandemic further accelerated the pace of digitization. In this context of tension between offering more services online to stakeholders and securing an increasingly adversarial environment, electoral stakeholders and democracy donors need to consider the cybersecurity risks associated with technological components, whether it is directly or indirectly related to the electoral process. Doing so in a piecemeal or ad hoc manner may not be sustainable, or sufficiently effective to counter current and future integrity threats. In this regard, lessons drawn from the larger cybersecurity industry – which emphasizes holistic management of cybersecurity – are applicable to the electoral space and should be embraced by the election community. Cybersecurity must be an ongoing process of risk management rather than a static requirement; mature cybersecurity programs are adaptable and continuously recognize threats and curate security mechanisms to address those threats through controls, vulnerability management, and continuous evaluation.

We recognize, however, that many EMBs may not currently be sufficiently resourced or positioned to enact such mature cybersecurity programs. The risk management frameworks used by governments and industry need to be adapted for the electoral space and further work must be done to tailor them to local contexts. While there has been a great deal published recently to advance thinking about the intersection of cybersecurity and electoral operations globally, there is still much more that needs to be done. At the national level, some countries are saddled with laws and regulations that effectively prevent electoral stakeholders from addressing emerging issues of the digital age. These issues are myriad and include assigning responsibility for protection of electoral infrastructure, standardizing security requirements, coordinating the flow of information across various stakeholders, and securing information against misuse while also anticipating and planning for response and resiliency. Cybersecurity must be considered at every stage of the electoral process, which is currently not the case in many countries. These considerations include implementing fundamental managerial controls such as policies that ensure procurement of secure

[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/

ICT-related solutions from reputable vendors. They also include operational controls of ICT-equipment and databases executed by employees, volunteers, and other related users that minimize risk. Finally, these considerations include how to best implement technical controls such as automated cyber defenses to help ensure security throughout the electoral process. Good practices are emerging and will need to be codified and circulated for the electoral community to further institutionalize adoption at national and local levels.

Safeguarding the practice of elections in the cyber era is not simple, as the electoral process varies significantly globally, as do the threat profiles. The institutions and stakeholders involved in elections often control elements of the information technology infrastructure independently; therefore, any compromise of confidentiality, integrity, and/or availability may have systemic effects across the electoral process that could undermine the entire election. There are practical steps EMBs, political parties, and civil society organizations, among others, can take to further mature election cybersecurity. While these practical steps begin with the education of users to exercise adequate cyber hygiene, they extend much further across all levels of electoral management. Incorporating modern security controls and practices will undoubtedly take time and resources while requiring further adaptation across democracies worldwide, each with their unique context and local intricacies.