JUNE 17, 2021

EVOLVING INTERNATIONAL ELECTIONS SECURITY FRAMEWORK

RYAN WALSH

The sanctity of elections is well established. But not just the sanctity of any kind of elections, it is free and fair elections that people demand. They want to know that when they cast their vote it means something. That their voice is being heard and is equal to that of their neighbors. As a result, elections must be free from interference from threats at home and abroad. In its most basic sense this can be understood to mean if a foreign power or domestic group physically changed votes both the freedom and fairness of a country's elections would be brought into question. But, with the advent of technology, this also means if a foreign power or domestic group used digital means to change or sway an election the freedom and fairness of an election would be brought into question as well. Thus, the security of elections, both physically and digitally, is paramount to both the administration of and perception of free and fair elections.

Helping to ensure the security of elections is what the Global Cyber Alliance Cybersecurity Toolkit for Elections does. But this toolkit is just one critical cog in a larger essential machine. This post will lay out the larger international framework around securing elections. It will utilize the United States as a case study and place the GCA toolkit within the framework. The reasons for the use of the United States as a case study are twofold. First, as the first nation to develop cybersecurity policies the United States is a key player in this area. Second, the 2020 U.S. election was a prominent test of current election security developments based on the safeguards that the United States has implemented after falling victim to an election interference campaign. While this post utilizes the United States as a case study, the framework is broader, made up of the following mutually reinforcing parts: the international laws/norms around election security, the government's role in election security, civil society's role, elections officials' role, and individuals' role.

The Starting Place: International Laws/Norms

Using The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means and starting at a high level and working to the national, the framework begins with the international order. The basis of the current international order is the United Nations Charter. States rights to sovereignty and self-determination are two important aspects of the Charter for this discussion. Taken together these rights ensure that a State has the right "to conduct its affairs without outside interference". Election interference is one example of this outside interference and, according to the Oxford Statement, election interference can also, "infringe human rights protected under the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights, and the European Convention on Human Rights". To understand State responsibility for election interference, "the International Law Commission's 2001 Articles on State Responsibility establishes that a state is responsible for the conduct of its organs or officials, as well as for conduct carried out by persons or groups acting on the instructions of, or under the direction or control of, the state". Ultimately, this combination of States rights, Human Rights, and States responsibilities manifests in States international legal right to and the emerging norms framework around free and fair elections.

While this is generally agreed upon, election interference has become more nuanced in the cyber realm with disinformation campaigns, hack and leaks, and the real threat of direct cyber-attacks on election infrastructure. While it seems that cyber-attacks on election infrastructure are illegal, being a violation of the rights mentioned above, international law has been slow to keep up regarding disinformation campaigns and hack and leaks. In these efforts the UN Group of Governmental Experts (GGE) has said, and NATO's Tallinn Manual 2.0 has pointed to the fact that international law is applicable in the cyber realm. Furthermore, according to the Oxford Statement referenced above,

> In line with the UN Guiding Principles on Business and Human Rights, online intermediaries and digital media companies should 'conduct due diligence to ensure that their products, policies and practices … do not interfere with human rights', as recognised in the April 2020 Joint Declaration on Freedom of Expression and Elections in the Digital Age, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression.

As a result, the case for all aspects of election interference being just as illegal in the cyber realm as it was before election infrastructure relied so heavily on technology, could be made.

Amongst international lawyers the discussion seems to now be about what specific principles of international law these more nuanced kinds of election interference operations violate. Whether these types of campaigns are acts of war, violations of sovereignty, violations of self-determination, or a combination of the three. The most compelling argument may be that these more nuanced kinds of election interference operations are illegal under international law because they violate the principle of self-determination. But the current underdeveloped nature of the application of international law to the use of information and communications technologies (ICTs) and the continued development of cyber norms have created two results regarding disinformation campaigns and hack and leaks. First, repercussions for these aspects, and election interference broadly, have usually taken place outside of the courtroom. With the legality being determined on a politically charged instance by instance basis. Second, these repercussions have used levers outside of the traditional judicial arm of governments with actions such as naming and shaming, sanctions on the individuals and country responsible, expulsion of diplomats, and even proportional retaliatory and or preemptive cyber attacks.

A range of organizations support the development of specific international norms and legal frameworks around election security. In the international landscape, across governments and civil society, the UN GGE, the UN Open Ended Working Group (OEWG), the Paris Call for Trust and Security in Cyberspace, and the Global Commission on the Stability of Cyberspace are evolving international cybersecurity norm building bodies. All these bodies put forth cybersecurity as a central tenant and a norm that must be supported, and some have specifically said the same about election security. While the UN GGE and UN OEWG have not used the specific term election security, they have supported international law and norms around cybersecurity that States could draw on to argue for the applicability of election security. For example, the UN GGE in A/68/98* and A/70/174 affirmed the applicability of international law and the UN Charter to States actions in cyberspace. Specifically, they affirmed the applicability of State Sovereignty and non-intervention, as well as norms around not attacking critical infrastructure. The UN OEWG, in its second draft of its report, affirmed the findings and recommendations of the UN GGE and is working to expand upon them. As referenced earlier both the Paris Call and the Global Commission on the Stability of Cyberspace have made election security a central pillar. The Paris Call made election security its third principle out of nine common principles to secure cyberspace. The Global Commission on the Stability of Cyberspace made election security its second norm out of eight proposed norms of responsible behavior in cyberspace. While these four norm-building bodies are ongoing efforts, and the representatives of the international community within them are disparate, they represent a committed effort in the international community to build norms and laws around election security.

Governments

Governments help develop these international norms and laws around election security, but their primary role is to secure their own elections. This is accomplished through the passage of domestic laws, the funneling of resources, and coordination with election security stakeholders. The passage of laws defines the rules of how elections will be held, sometimes how elections will be secured, and sometimes the repercussions from malicious election interference. The funneling of resources directs Government money, policies, agencies, personnel, and messaging towards securing elections. Whether that be implementing cyber and physical security into election infrastructure, actively combatting election interference campaigns, or imposing costs on the perpetrators of those campaigns. Lastly, the coordination with election security stakeholders involves working with election officials, civil society, society more broadly, and individual voters to ensure elections are conducted in a free and fair manner.

Moving to individual governments, in the United States, the federal government's efforts to secure elections domestically helps to ensure the implementation of international laws and norms around elections domestically. While most of the responsibility for conducting and securing elections falls to the states and local governments, the federal government, in particular the legislative and executive branches and the Federal Election Commission, plays a critical role. Congress has worked to secure elections through laws such as the Help America Vote Act (HAVA) of 2002, the Fiscal Year 2020 National Defense Authorization Act, and the Coronavirus Aid, Relief, and Economic Security Act (CARES) of 2020. These laws and others like it have created agencies like the Election Assistance Commission (EAC) and directed funds towards these and other sectors of government that are responsible for ensuring election security. Further, through the Defending the Integrity of Voting Systems Act of 2020 Congress broadened the language of the Computer Fraud and Abuse Act (CFAA) of 1986 making it illegal to hack a federal voting system. This act serves as both a deterrent for potential attacks on the electoral infrastructure and as a means through which the U.S. federal government can impose costs as well as seek redress in the event of this kind of attack.

Historically federal agencies have drawn direction for combating foreign election interference, increasing cybersecurity efforts, and securing elections from official executive actions. In the United States these actions often come in the form of Executive Orders (EO) and Presidential Policy Directives (PPD) that have been written and sometimes rewritten across administrations. The actions that follow from these orders and other informal and formal directions represent a whole-of-government approach that is needed to secure elections.

Safeguarding Your Vote: A Joint Message on Election Security explains the federal actions that have resulted from these executive directions. Federal law enforcement, in the United States this is the FBI, being the "primary investigative agency responsible for malicious cyber activity against election infrastructure, malign foreign influence operations, and election-related crimes, like voter fraud and voter suppression”. Government military and intelligence agencies, like U.S. Cyber Command and the NSA, work to “generate insights, enable defenses, and, when authorized, impose costs on foreign adversaries”. Domestic security agencies, like the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS), are “focused on securing our nation’s critical infrastructure and the essential services that underpin our society”. Election infrastructure being one of the sectors designated as critical infrastructure in the United States. They also “help make the election systems across the country as secure and resilient as possible…[and] work to increase audit-ability of voting processes, including the vote itself”.

Other broader efforts have resulted from these policy initiatives as well. With the short supply of cybersecurity election expertise, the National Guard has worked to fill the gap. In regards to campaigns, the FBI’s Protected Voices initiative provides support to political campaigns, companies, and individuals to combat online foreign influence operations and cybersecurity threats as a result of these executive actions. Also, the Federal Election Commission Advisory Opinion 2018-11 allows Microsoft in particular, and further opinions have allowed other private entities, to provide political campaigns with cybersecurity products and services to aid in election security. In total all of these disparate efforts come together through intelligence sharing and collaboration between federal agencies, the federal government and the private sector, and the federal government and local governments to result in a whole-of-government approach to election security.

Civil Society

Civil society provides the next step in securing elections through a range of multi-stakeholder processes that have provided research, resources, recommendations, playbooks, and toolkits that support election officials and campaigns in turning the steps to implementing election security into practice. An example of this is the Center for Internet Security’s Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC provides the election subsector with tools, real time intelligence, training, resources, and expertise for securing elections through collaboration and information sharing among its members, DHS broadly and CISA specifically, other federal partners, and private sector partners.

These civil society processes have also resulted in election security playbooks, controls, and toolkits that touch on every aspect of securing the election process. Three such examples of these playbooks and controls are the Belfer Center: State and Local Election Cybersecurity Playbook, the Belfer Center: Cybersecurity Campaign Playbook, and the Center for Internet Security: A Handbook for Elections Infrastructure Security. There are also more nuanced playbooks that focus on securing specific parts of the election infrastructure or address specific issues about current elections. These include things like the MITRE: Recommended Security Controls for Voter Registration Systems and the Brennan Center Report Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials. Finally, to bridge the gap between research and practical implementation of security, an election security checklist and toolkit have been created. GCA has created the Cybersecurity Toolkit for Elections and the Center for Internet Security has a similar Elections Security Checklist, which also supports implementation of their handbook. Election officials can use these resources to implement the technological tools necessary to achieve election security in practice.

The Last Mile: SLTTs, Election Officials, and the GCA Toolkit

This final step is in many ways the most crucial in all the process. This is where the process goes from at times aspirational policy to operational reality. Through the use of the GCA Cybersecurity Toolkit for Elections, election officials can implement all of the goals in each of the previous sections of the above-described framework. In the United States this takes place at the State, Local, Tribal, and Territorial (SLTT) level. Through use of the toolkit election officials can implement many of the recommendations set forth by the playbooks, reports, ISACs, and controls for election security mentioned above. Through use of the toolkit the Government's goal of securing elections can be realized. All the funneling of resources, passage of laws, and direction of federal agencies can see their efforts come to fruition. The federal government can assure the people before, during, and after elections that the efforts they have taken have been successful and that when they vote they can do so with the knowledge that the elections are secure. Lastly, the international norms and laws surrounding cybersecurity in elections can be realized. Democracy, self-determination, sovereignty, the rejection of foreign election interference, and ultimately the sanctity of free and fair elections can be better assured when the systems that support these processes are secure. That is where the GCA Cybersecurity Toolkit for Elections sits. Between the desire for elections security and elections official's practical implementation of that desire in reality.

Individuals Voters

There is one last cog in this framework that is often overlooked, individual voters and their role in security. The discussion around individual voters has been placed after the earlier discussion because individual voters don't play a direct role in the administration of election security but still play a critical one, exercising their right to vote and doing so responsibly. To fulfill this responsibility, they need to first understand that they are the main targets in malicious foreign interference campaigns. Second, in order to avoid falling victim to these influence operations they need to know how to seek out reliable information about elections. They can find this information through their state's official election website, verified campaign and election official pages, and viewing credible news sources with a critical eye. While looking for this reliable information voters can use protective cybersecurity measures, like Quad9, to ensure they are not visiting malicious websites. Next, individuals need to utilize this information to ensure they are registered to vote, know when and how to vote, and are utilizing reputable information to form their opinions. While this will not protect them completely from disinformation it will provide them with reliable information to counteract it.

Once voters have taken these steps, they need to take the most important one, exercising their right to vote. This step is the most important for the following reasons. Election interference operations often don't seek to physically change votes that would change the outcome of an election in any significant way. These operations usually seek to manipulate who individuals vote for or, more dangerously, create the appearance of a fraudulent or manipulated election in order to weaken individuals beliefs in Democracy to the point they do not exercise their fundamental right to vote. But the principle that through voting the power is with the people is what Democracy is founded on. Thus, the importance of individual voters in the election security framework is because if individual voters are manipulated in their voting choices or completely lose faith in the system itself, demoralized to the point of not voting, then over time the erosion of citizens' faith in the electoral process threatens the very fabric of Democratic societies. Securing this faith, in sum, is what the entire election security framework's efforts are for.

Where To Go From Here

The election security framework described in this piece is evolving into a concrete and sustainable solution to the modern problems of election interference. In this evolution, the 2020 U.S. election was a test for the efficacy of this framework and it was one that a coalition of election officials declared passed. While the framework held and the security of the election was ensured, there is more that needs to be done. Lessons from this election need to be applied to future elections around the world in a sustainable fashion. Additionally, while progress has been made to address the issue of election security, this issue will evolve. Adversaries will develop new tactics that will need to be continually addressed. But these developments will not challenge the foundations of the framework. These new developments will merely bring new questions about how specific aspects of the framework will apply.

More importantly the 2020 U.S. election and the events in the U.S. Capitol on January 6th, 2021 made clear the problem is no longer solely confined to defending against foreign malign influence. The substantial threat of domestic disinformation campaigns is an issue that is beginning to be grappled with and needs to be incorporated into this framework as well. Measures to combat domestic disinformation campaigns may be an even harder aspect of the framework to develop though. This increased difficulty is because it is easy to rally to defend against a foreign enemy, but it is much more difficult to come together and combat a problem that originates from within. The election security framework offers a part of the solution to this problem already though. The implementation of this framework provides election officials with the capability to point to cybersecurity controls and auditability in election processes. By showing their work election officials can counter disinformation narratives that seek to erode confidence in the legitimacy of elections. This approach is effective, but it is only one aspect of the solution to the problem of domestic disinformation campaigns and the election security framework needs to build upon it in the following ways.

First, the framework needs to build on and improve its messaging so election officials can show their work more effectively. Efforts like the FBI protected voices, CISA Rumor Control, the declaration by the coalition of election officials, and civil society efforts like the Election Integrity Partnership need to be expanded, improved, and emulated internationally. Further, concrete solutions need to be developed and implemented to reach those who have fallen victim to these campaigns and will consequently be less trusting and harder to reach. Through a committed effort to spread truthful election security information, throughout the entire media ecosystem, the electorate can be better made aware of the true state of election security. Helping to better combat and reduce the effects of and susceptibility to these campaigns.

The second way the framework should build on its efforts is through improving capabilities for identification of disinformation campaigns at multiple layers of the framework. Identification is essential to providing an informed picture of these campaigns for those who are responsible for combating them as well as helping the electorate spot disinformation themselves. The framework should expand, improve, and emulate efforts already undergone at the civil society, election officials, and government layers of the framework. Things like MITRE SQUINT, the Election Integrity Partnership, FBI protected voices, and social media companies work during the 2020 U.S. election to spot and fact check election disinformation are good first steps and need to be built on. A committed effort for providing the electorate with the skills and tools to identify disinformation needs to be built as well. This includes educating voters on media literacy and tactics for spotting disinformation. Further, civil society should work to develop and spread technical solutions to help individuals combat and spot election disinformation. Microsoft created two new tools to detect manipulated content already, the Microsoft Video Authenticator and a combined certificate and reader. User friendly versions of these tools should be adopted widely, more solutions like them should be developed, and they should be packaged together in disinformation defense toolkit solutions like GCA's Cybersecurity Toolkit for Elections.

The last way the framework should build on its efforts is through developing ways of holding those responsible for domestic disinformation campaigns accountable. This accountability can be built into multiple layers of the framework. To begin with, social media companies are the ones who play the most significant role in moderating disinformation campaigns and their efforts should be incorporated in the framework going forward. They have developed election disinformation policies, consequences for violating those policies, and enforcement mechanisms for those consequences. The 2020 U.S. election was a significant test for these policies. By drawing on lessons learned from this test and through continually improving these policies so that they are clear, effective, and consistently enforced they will be better equipped to address the challenge in the future. At the government layer, there needs to be accountability for government officials and those seeking to be government officials who conduct domestic election disinformation campaigns. Accountability for these individuals needs to include a range of consequences that at its most severe includes removal from or disqualification from office and legal liability. It cannot be overstated the importance of holding government officials accountable for conducting election related domestic disinformation campaigns. Not only are they violating their duty, but these individuals are best positioned to most effectively conduct these kinds of operations and inflict the most damage.

These improvements and the efforts of the election security framework as a whole are essential. One need only turn to the domestic disinformation campaign that sought to question the security and legitimacy of the 2020 U.S. election and culminated in the violent events in the U.S. Capitol on January 6th, 2021 to understand why. Ultimately, though, the security of the 2020 U.S. election should provide hope for the capabilities of the emerging election security framework to address these new challenges and serve as a means to ensure the sanctity of free and fair elections in the future.