Protecting Elections

As a Matter of National Security

Gregory Miller
Co-Founder, COO

Sergio Valente
Election Technology Policy Analyst, Office of the CTO

OSET INSTITUTE

March 2018

March, 2018

About the OSET Institute

The OSET ("Oh-Set") Institute is a 501(c)(3) tax-exempt, nonpartisan, purpose-based election technology research corporation chartered with research, development, and education in election technology innovation.

The Institute's flagship effort, the TrustTheVote™ Project, is developing **Elect**OS™ a next-generation, higher integrity, lower cost, easier-to-use election administration and voting technology framework freely available for any election jurisdiction to adopt and have professionally adapted and deployed. ElectOS and all open source election technology is being designed and engineered per the requirements and specifications of election officials, administrators, and operators through a Request For Comment (RFC) process.

As part of our research, development and education mission, from time to time, the Institute produces Briefings, Essays, White Papers, and other content to inform stakeholders, supporters, and the public about issues of election technology innovation and integrity.

Threats to our election administration technology infrastructure are inherently threats to our democracy.

March, 2018

Table of Contents

OSET Institute Supporter Acknowledgement

The OSET Institute deeply appreciates the **John S. and James L. Knight Foundation**, the **Democracy Fund**, the **Frost Foundation**, the **James H. Clarke Foundation**, the **Chris Kelly & Jennifer Carrico Family**, the **Barbara Coll Family**, the **Michael L. Henry Family**, **Matt Mullenweg**, the **Frank J. Santoro Family**, and the **Aleksander Totic Family** for their generous support of our work to increase integrity, lower cost, and improve usability of election technology infrastructure in the U.S. and abroad.

March, 2018

Executive Summary

Elections are an issue of national security. They represent a sovereign act of the American people as they express their right to self-determination and to choose their desired government. As a sovereign act, elections are expected to be an entirely domestic affair, free of foreign intervention. Any such intervention would be an affront to American sovereignty. But intervention in elections is a complicated issue that can take many forms. While a disinformation campaign might still violate national sovereignty, it is distinct from an attack that directly alters vote tallies, and these two types of attack require different responses. There are three categories of attacks on elections: *subversion*, *defamation*, and *disruption*.

Evaluating the nuances of these different attacks is critical for determining the proper, and proportional response. Russian interference in the 2016 election raised questions about whether *cyber attacks* constitute an act of war, or state interference, or whether they warrant any kind of retaliation. If retaliation were warranted, what kind of retaliation would be justified? Individual nations as well as multinational groups such as the European Union, North Atlantic Treaty Alliance, and the Organization for Security and Cooperation in Europe are still debating these questions. Discussion must continue so that a more universal understanding of the consequences of cyber attacks and appropriate responses can be developed, because these attacks will not stop.

Elections are a national security interest, but election operations are the purview of state and local governments. The importance of characterizing elections as a national security matter is that it encourages policymakers to prioritize their security and integrity; it is a recognition that for America to protect the rights and independence of its citizens it must protect their ability to express their will, free of foreign interference. There is no reason why this reprioritization needs to come at the cost of states' rights and their ability to administer elections independent of the federal government. This is not a call for FBI agents or Department of Homeland Security personnel to be placed in voting booths, as some thought-leaders fear.[1] It is rather a call to increase attention to (and funding for) the fundamental vulnerabilities[2] of election technology, and to increase the ability of states to access the resources necessary to improve the security of their election systems.

---

1 Hans A. von Spakovsky. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?" *The Heritage Foundation*, August. 17, 2016, www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure.

2 Gregory Miller, John Sebes, and Joy London, "Critical Democracy Infrastructure," *OSET Institute*, September 2017, http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure.

1. Introduction

The 2016 election cycle highlighted both the importance and the vulnerability of America's election technology infrastructure. As time passes, new information about the extent to which the Russian Federation employed a disinformation campaign in an effort to influence American elections is being discovered and vetted. To recap, the Russian Federation's actions included at least:

- The conveyance of stolen information (primarily eMail) to WikiLeaks;
- The creation of illegitimate ("fake") social media accounts;
- The deployment of automatic information dispersement Apps ("Bots");
- The development and publication of falsified news stories intended to sway attitudes, beliefs, and perceptions in specific memes;
- The purchase and finely targeted placement of political advertisements; and
- The malicious probing of American voter registration systems in at least 21 states and in two cases successful penetration of the registration databases.[3]

All of this has led to concern of the American people, and policymakers, who face the daunting question of what must now be done to solve this flagrant violation of American sovereignty.

However, this paper is not concerned with what took place durig the 2016 presidential campaign, but rather with what should be done going forward to improve the security of our election technology infrastructure. At this point, we need to draw a clear distinction in that regard. Election technology infrastructure, in general, concerns all of the technology applied to the administration and operation of elections, and may in some circumstances and scenarios concern campaign management and electioneering. The latter is out of our scope of research, study, and innovation efforts. We are focused on the former—that which powers the administration and operation of elections and not the process of campaign management or electioneering.

Regardless of whether, or to what extent the most recent American election was actually manipulated on either side of the ecosystem (i.e., administration/operation or campaign management/electioneering), there is evidence that elections have the clear potential to be manipulated. That alone should be cause for concern.[4]

---

[3] Sari Horwitz, Ellen Nakashima and Matea Gold, "DHS tells states about Russian hacking during 2016 election," *Washington Post*, September 22, 2017, www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.c86030dfa7e5.

[4] Robert Schlesinger, "Hack the Vote: a reminder of how insecure our ballots can be," *U.S. News & World Report*, July 31, 2017, www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are.

2. Sovereignty and Security

U.S. elections are American citizens' most basic expression of self-determination, their ability to choose their own government, to affect the policies of their nation, and to establish the consent of the governed.[5] There is also the right to self-determination of election officials, or those who choose to run for election. Politicians have the right to run in races and represent constituents' interests, free of foreign meddling.

In addition to being an expression of self-determination, elections are a sovereign act, one that, at least in theory, is free of foreign intervention. The Westphalian system,[6] along with the UN Charter and other international agreements, protect nations' rights to exclusive dominion over their domestic affairs. While exceptions might be made for extreme events such as genocide, the elections of a nation, particularly free and fair elections, are protected as a sovereign act. In America, this is an act over which the citizens and their states should have exclusive control. Nations also have an obligation to provide for the security of their citizens. Governments have a responsibility to their citizens to provide national security, and protect critical infrastructure, and maintain the physical security of its citizens. However, before any nation can guarantee these obligations its' legitimacy must first be secured. In the U.S. that legitimacy stems from its elections and the belief that they are free and fair. Therefore, the American government has an obligation to ensure that its elections are *actually* free and fair, and for elections to be free and fair, they must be free from foreign interference.

However, if this philosophical reasoning is not enough, public confidence in elections can be linked back to national security. As America learned during the Vietnam War, the success of military operations often rests on how much public support they receive. For the public to support its government's national security efforts it must also have faith that the government representing them is legitimate.[7] It is also plausible (though presumed unlikely) that election interference by foreign states *could* cause officials to be elected who support policies that run counter to America's national interests and security, or that disinformation campaigns *could* alter the national discourse surrounding national objectives in such a way that they are undermined.

Foreign intervention in a U.S. election would then logically be a violation of American sovereignty. As Rudi Mehrbani from the Brennan Center for Justice stated, "*The Russians' [actions during the 2016 election cycle] were rightly considered a violation of states'*

---

5 "Handbook on Observing and Promoting the Participation of National Minorities in Electoral Processes," *Organization for Security and Co-operation in Europe*, 2014, www.osce.org/odihr/elections/124067?download=true.

6 See: https://en.wikipedia.org/wiki/Westphalian_sovereignty

7 Bruce Fein, "Elections security is national security: Graham-Klobuchar amendment to NDAA is imperative," *Washington Times*, August 28, 2017, www.washingtontimes.com/news/2017/aug/28/elections-security-national-security/

sovereignty and an affront to the most fundamental of democratic processes — voting."[8] To some, this might appear to be an act of war. U.S. lawmakers, such as Sen. John McCain (R-AZ) and Rep. Bonnie Coleman (D-NJ), among others have endorsed this view.[9, 10] While there is no consensus on how foreign election interference should be characterized, the perception that our elections are a matter of national security is gaining prominence.

The rationale for this claim is quite simple, but other concerns complicate the matter. Any violation of American sovereignty is perceived to be an attack against the U.S., although there are certainly different *tiers* of attacks. The question then becomes: *What does this mean*? Critics of such a viewpoint are quick to point out that elections, regardless of their importance to national security, are a matter for the 50 states, not the federal government. Disregarding the federalism question of elections, there is reason for every American to be concerned about the consequences of federal management of elections. Many state and local elections officials worry that it would be all too easy for those in power to use national security as a justification to tilt the scales of an election in their favor.[11]

3. Avenues of Attack

To understand what the designation of elections as a matter of national security would look like, it is necessary to understand what elections would face in the current threat environment. The 2016 Russian incident made clear how real the threat is, and the information Russians gained through their interference, as well as the vulnerabilities exposed, can (*and will*) be leveraged by other actors, including the nation-states Iran, China, and North Korea. Policymakers must consider the potential for these actors to weaponize America's electoral process and sow political chaos and polarization—*which is their primary objective, rather than affecting the outcome in favor of one candidate over another*. In fact, their goal is to derail an election to the point of at least undermining the legitimacy of a winner, or at worst, it being impossible to ascertain any winner. The stakes are high, and Americans cannot afford to sit idly by as foreign adversaries manipulate our domestic affairs; Americans must recognize election integrity for the national security issue that it is and take steps to improve election security.

---

8 Rudy Mehrbani, "States: Seize this Moment to Compel Congress' Help in Shoring Up Voting Systems," *Brennan Center for Justice*, November 10, 2017. www.brennancenter.org/blog/states-seize-moment-compel-congress-help-shoring-voting-systems.

9 Theodore Schleifer and Deirdre Walsh, "McCain: Russian Cyber-intrusions an 'Act of War,'" *CNN*, December 20, 2016, www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html.

10 Morgan Chalfant, "Democrats step up calls that Russian hack was act of war," *The Hill*, March 26, 2017, thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war.

11 Pam Fessler, "State And Local Officials Wary Of Federal Government's Election Security Efforts," *National Public Radio*, April 5, 2017, www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts.

Cyber attacks are a complex issue. Attacks can be domestic or international, the implications of which can vary greatly. There are broadly three kinds of attacks on elections: subversion, defamation, and disruption.

1. **Subversion attacks** encompass the types of attacks that are often discussed by media outlets, and they are those that first come to most people's mind when thinking about attacks on elections. Such attacks involve manipulating and altering vote tallies in order to change the result of an election. There is a tendency to exaggerate both the prevalence of subversion attacks and conversely, to underestimate their ability to succeed. Subversion attacks are relatively uncommon, and there was no evidence that they took place in the 2016 election cycle.[12] However, many also assert a misperception that America's election infrastructure is safe from this sort of attack due to the diversity and wide distribution of the systems.[13] It is true that the U.S. has several types of voting systems, but there are only about 5-6 distinct variations, and while this makes it more difficult to infiltrate American elections, it does not make it impossible. In fact, in order to change the outcome of a national election, significantly fewer votes need to be changed in order to affect the margin of victory in swing states.[14]
2. **Defamation attacks** are attacks that de-legitimize elections by creating distrust within the domestic population. Foreign or domestic actors might employ disinformation campaigns by cyber operations in order to carry out defamation attacks. Social media campaigns that spread false information is onr example. A malicious actor could also launch a cyber attack that alters vote tallies (or election results prior to publication) in such a way that it would be obvious the results were altered, thus creating distrust within the American people. These attacks might be aimed at giving a one candidate an advantage, or, more likely, simply at sowing division and disorder.
3. **Disruption attacks** seek to impede the electoral process, for instance, preventing eligible voters from casting a ballot, with the intent of either altering the result of the election or creating accusations of voter suppression. For example, an actor could manipulate voter registration databases to change voter information (such as their address or party affiliation) to render them unable to vote in an upcoming election. The voter information could eventually be corrected, but it would take time, likely

---

12 To be precise, it was impossible to determine, let alone prove the occurrence of this type of an attack, because the steps necessary to conduct the level of digital forensics required were never taken for a variety of reasons. Thus, not only was there no concrete evidence, there was no effort to make such an examination and analysis.

13 "Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra," *The Department of Homeland Security*, June 21, 2017. www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

14 Tim Meko, Denise Lu, Lazaro Gamio. "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016. www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

leading to affected voters choosing not to vote or at least to increased wait times at polling booths. Similar to subversion attacks, disruption attacks, if directed at specific precincts in swing states could alter the result of a close election. Or, even if they didn't change the result of the election, they could breed suspicion that either the states or the federal government was engaging in voter suppression.

4. Legality of Avenues of Attack

The importance of these three differentiated avenues of attack is not just that understanding them is critical to the task of improving the security of our election system and infrastructure, but additionally, and more relevant to the scope of this paper, that they are different in the legal sphere.

Subversion and disruption attacks can generally be grouped together in a legal sense as they both involve the direct manipulation of voting systems. A disruption attack that involved changing vote tallies in an obvious way would also fall under this umbrella. These attacks are *illegal*. It would be illegal for a domestic actor, whether a private voter or a public servant, to take any of these actions. Foreign actors would also be prohibited from any form of direct manipulation.

While any form of manipulation of vote tallies is certainly illegal, disinformation campaigns are a more complex issue. At the end of 2016, fears that Russia had used propaganda to influence the outcome of America's election led to the introduction of the Counter Disinformation and Anti-Propaganda Act. This bill declared not only that Russia had used large-scale disinformation campaigns to destabilize American interests, but also that these acts undermined America's national security.[15] The bill was eventually passed as a part of the National Defense Authorization Act for the 2017 fiscal year. Since the Act establishes that disinformation campaigns undermine national security it becomes clear that protecting our elections from these attacks is an issue of national security.

5. The Democracy Ecosystem

The question then becomes: *What to do about the security of American elections*? There are many steps that can be taken to improve the security of American elections from results manipulation. The Department of Homeland Security designation of election infrastructure as critical infrastructure in 2017 may play an important role in helping to facilitate these needed improvements. Other papers have covered this topic at length.[16]

But there is far more to elections than just the voting machines and voter registration databases. Mainstream media, political party committees, and social media outlets are all part of what we might term the broader *democracy ecosystem*; all are critical to the operation and legitimacy of an election, yet don't directly involve the casting of ballots.

---

[15] Adam, Kinzinger. "Text - H.R.5181 - 114th Congress (2015-2016): Countering Foreign Propaganda and Disinformation Act of 2016," *Congress.gov*, May 10, 2016, https://www.congress.gov/bill/114th-congress/house-bill/5181/text.

[16] Gregory Miller, John Sebes, and Joy London, "Critical Democracy Infrastructure," *OSET Institute*, September 2017, http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure.

Any realistic view of election security must recognize that all these factors need to remain unimpeded for an election to be legitimate. The hacking of the Democratic National Committee[17] and the disinformation campaigns run by Russia during the last election cycle all contributed to a weakening of faith in American elections.

The U.S government has an obligation to try to secure the integrity of elections. However, strict regulation of political parties and news organizations would severely weaken the political independence of our election system, which would in turn also damage Americans' faith in their elections. In order to maintain the independence of domestic political actors while protecting them from foreign interference, federal and state governments can provide access to best practices, information sharing, and resources so that these organizations can best protect themselves from foreign interference.

This leads to the important distinction to be made in the realm of disinformation campaigns between foreign and domestic actors. It may be hard to determine a legal difference between a disinformation campaign and any attempt to affect the views of the electorate, which is deemed permissible for U.S. citizens. Campaign contributions, and the advertisements they pay for, are one clear example of how citizens, and corporations, are allowed to try to influence voters' thoughts and opinions. This may not be that different in a legal sense from creating fake social media accounts to support various viewpoints. There is no attempt to coerce voters into casting their ballots in a specific manner or to artificially increase the vote tally for a particular candidate. Disinformation campaigns only use words, which is perfectly legal for U.S. citizens.

However, even if it might be permissible for a domestic actor to take these actions, elections are fundamentally a sovereign act among the people of a nation. International observers might at times be welcomed and encouraged to monitor an election, but not to try to influence the result. The Federal Elections Commission has clear restrictions about how foreign nationals can legally interact with an American election. For example, unlike U.S. citizens, foreigners are *prohibited* from making campaign contributions or other forms of donations that might affect an election.[18] Any disinformation campaign from a foreign government is arguably *illegal*.

Even if these disinformation campaigns are illegal, it is not necessarily easy to find a solution. For an election to be legitimate it must be an activity, independent of both foreign interference and domestic interference by the federal government. There is an expectation of transparency that can come into conflict with the interests of national security. Herein lies the heart of this issue: *How can America protect its elections, an issue vital to American sovereignty and national security, while maintaining their independence*?

---

17 Timothy Lee, "DNC email leaks, explained," *Vox*, July 25, 2016, https://www.vox.com/2016/7/23/12261020/dnc-email-leaks-explained.

18 "Foreign Nationals," *Federal Election Commission*, June 23, 2017, https://www.fec.gov/updates/foreign-nationals/.

6. Improving Election Security

Policymakers must consider the domestic reforms [19] needed to make American election systems less vulnerable to cyber attacks. It is critical that these reforms do *not* come at the expense of the 10th amendment and states' rights to administer elections in an independent manner. However, the federal government can help by increasing the ability of states to access the necessary resources to improve election security.

Neither the founding fathers, nor the vast majority of policymakers over history, were particularly concerned with the security of American elections, and at the time, for good reason. The advent of cyber attacks and integration of computers into election systems greatly increased the potential for election manipulation in a way that was not conceivable before. The procedures to prevent ballot-box stuffing share almost nothing with those aimed at preventing cyber attacks or more nuanced election manipulation. Disinformation attacks, such as character assassinations, dating back to just the 18th century, have nothing close to the reach and impact of 21st century social media campaigns.

The critical infrastructure designation offers one important way to improve election security within the existing framework of election administration and operation. The designation aims to free up additional resources for election cybersecurity and to create information sharing systems (such as Information Sharing and Analysis Organizations) to facilitate security improvements, while ensuring that all participation is voluntary.[20] Legislators have introduced bills like the SAFE Act, which allocates funds for states to improve the security of their voting systems.[21]

Implementing mandatory security standards for elections is another option, but it is likely to be unpopular. Instead, the reprioritization of elections as an issue of national security is more likely to have the effect of increasing the awareness of lawmakers, both at the state and federal levels, as well as election officials, of the importance of election security and the threats posed to it. Our nation's election infrastructure is falling apart as the equipment on which it is based decay over time and counties lack the funds to replace them.[22] Correctly framing this deterioration of equipment as a matter of national security

---

19 An important consideration is the difference between tactical and strategic reforms. Both states' and federal agencies are working diligently to take all possible steps to mitigate at least, if not remove security vulnerabilities in current processes and platforms. However, there are imperative strategic reforms required to reinvent America's election technology infrastructure to ensure it is verifiable, accurate, transparent, and above all as secure as possible. This requires both a top-to-bottom redesign of the hardware and software of voting systems, and implementation of a secure and trustworthy supply chain of components and parts used in all voting systems.

20 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, Jan 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

21 "H.R.1562 - SAFE Act," March 16, 2017, www.congress.gov/bill/115th-congress/house-bill/1562/text.

22 Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk," *Brennan Center for Justice*, September 15, 2015, www.brennancenter.org/publication/americas-voting-machines-risk.

may serve to expedite efforts to remedy it and to invest in the innovation required to create systems that are not built upon architecture that is fundamentally vulnerable to manipulation.[23, 24]

7. The Proper Response

The next question is: What should be America's response to foreign interference in elections? Some Senators have called Russia's actions an act of war, [25] but there is a great deal of disagreement and uncertainty about how nations should best respond to cyber attacks. An article in the *New York Law Journal* by Benjamin Dynkin, Barry Dynkin & Daniel Garrie argues that Russian interference in the 2016 U.S elections is best classified as "state interference," rather than an "act of war."[26] The authors observe that an *act of war* has a clear and specific meaning in international law. According to Article 2(4) of the United Nations Charter that definition is:

> "*The threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations*." [27]

Election interference certainly does not violate the territorial integrity of a state, but it could be construed as violating a State's political independence. To evaluate this claim the authors turn to the Tallinn Manual, an academic study on how international law applies to cyber warfare, which states that "*cyber psychological operations intended solely to undermine confidence in a government* [...] [do] *not qualify as a use of force*." [28] According to this definition from the Tallinn Manual, direct vote manipulation, such as subversion or disruption attacks, *would* constitute an act of war, but the defamation attacks would *not*.

According to Dynkin et al, a better way of describing the disinformation campaigns carried out by foreign entities in the 2016 election cycle would be "state interference." State interference is a term that encompasses actions that interfere with with the affairs of a state and are coercive in nature. The meaningful distinction between state interference and acts of war comes down to their expected, proportional consequences. A proportionate response to an act of war could be a commensurate act of war, either in

---

23 See supra, Footnote 19

24 Gregory Miller, John Sebes, and Joy London, "Critical Democracy Infrastructure," *OSET Institute*, September 2017, http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure.

25 Theodore Schleifer and Deirdre Walsh, "McCain: Russian Cyber Intrusions an 'Act of War,'" *CNN*, December 20, 2016, www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html.

26 "Hacking Elections: An Act of War," *New York Law Journal*, June 5, 2017, www.newyorklawjournal.com/id=1202788705366/Hacking-Elections-An-Act-of-War.

27 "Article 2(4)," *The United Nations Charter*, legal.un.org/docs/?path=../repertory/art2/english/rep_supp3_vol1_art2_4.pdf&lang=EFS.

28 "Tallinn Manual on the International Law Applicable to Cyber Warfare," *Cambridge University Press*, 2013, www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

conventional or cyber form. This might involve missile strikes, troop deployment, or comparatively aggressive measures when compared to state interference, which might be responded to with sanctions or the expulsion of diplomats.

However, the tenets expressed in the Dynkin et al article are not the only voice on how cyber attacks should be interpreted. The EU has launched a recent initiative titled "*The Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*," which creates a "toolbox" of diplomatic responses to cyber activities that fall short of military action. The EU intends the framework to work as a deterrent against what it terms as "*malicious cyber activities*" and it was created in response to Russian cyber activities, but it remains unclear how the framework will be applied and whether or not it will prove an effective tool.[29]

The Organization for Security and Cooperation in Europe (OSCE), a 57-state organization that includes the U.S., has also made declarations about how to respond to cyber attacks. In the 2017 Minsk Declaration the OSCE reaffirmed what it had previously stated in the Astana and Oslo Declarations:

> "*Cyber attacks against vital state and commercial infrastructure are equivalent in nature to those of a conventional act of aggression*." [30]

While the OSCE does not discuss the specific issue of cyber attacks on elections, it creates a clear standard for how cyber attacks in general should be addressed.

There is no consensus yet on the legal nature of cyber attacks on elections. For America, it is vital that organizations and governing bodies such as the National Security Council (NSC) and the U.S. Congress continue this discussion and determine what the proper response to election manipulation by foreign actors should be going forward. In the meantime, much can be done outside of legal frameworks to improve America's resiliency and security against such attacks.

8. Conclusion

The integrity of American elections has serious implications for the security of the U.S. In order for America to maintain its sovereignty and to be functionally independent, it must ensure that its elections remain a domestic and sovereign affair, unmolested by any foreign interference.

While this premise might be agreeable to most policymakers, the implementation must be done with cautious prudence and with care for the institutions involved. There is an inherent risk and fear that protecting from foreign intervention could trade off with the independence of domestic political institutions from the federal government. Policymakers must traverse a fine line between protecting the integrity of American

---

29 Sico van der Meer, "EU Creates a Diplomatic Toolbox to Deter Cyber Attacks," *The Council on Foreign Relations*, June 20, 2017, www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks.

30 "Minsk Declaration and Resolutions," *Organization for Security and Cooperation in Europe*, July 9, 2017, ccdcoe.org/sites/default/files/documents/OSCE-170709-MinskDeclaration.pdf.

elections while not violating that integrity themselves. Federal action must be executed *without* any compromise of the election responsibilities and powers of the states. States must always maintain the freedom of choice in how they administer and conduct their elections.

The OSET Institute believes the best way for policymakers to achieve this balance is to offer, but not compel acceptance of assistance. By reprioritizing elections as an issue of national security, policymakers can make possible more resources to research and adopt election systems that are more secure than those present in the status quo. Policymakers can also enable information sharing and analysis organizations (ISAOs) to help election officials make the best possible decisions.

Both election officials and political institutions have incentives, internal and external, to protect themselves from foreign intervention. If policymakers can offer them the means to protect themselves they will be able to do so independently and thus maintain the integrity of American elections at a domestic and foreign level.

In any event, America should never waiver from its commitment to protect our elections as a matter of our national security. The OSET Institute believes that such resolve is a moral imperative, and foreign acts of intentional interference with American elections (and it's sovereign right to free and fair elections) should be considered equivalent to a conventional act of aggression, and treated accordingly, albeit proportionally. How and what steps should be taken to protect against such aggression and how and what a proportional response should be are imperative topics for consensus-building.

Citations

1. Chalfant, Morgan. “Democrats step up calls that Russian hack was act of war.” *The Hill*, March 26, 2017. thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war.
2. Fein, Bruce. “Elections security is national security: Graham-Klouchar amendment to NDAA is imperative.” Washington Times, August 28, 2017. www.washingtontimes.com/news/2017/aug/28/elections-security-national-security/
3. Fessler, Pam. “State And Local Officials Wary Of Federal Government's Election Security Efforts.” *National Public Radio*, April 5, 2017. www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts.
4. “Foreign Nationals.” FEC.gov. Accessed October 8, 2017.www.fec.gov/updates/foreign-nationals/.
5. Gregory Miller, John Sebes, and Joy London, “Critical Democracy Infrastructure,” *OSET Institute*, September 2017, www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure.
6. “Hacking Elections: An Act of War.” New York Law Journal. Accessed October 8, 2017. www.newyorklawjournal.com/id=1202788705366/Hacking-Elections-An-Act-of-Wa.
7. “Handbook on Observing and Promoting the Participation of National Minorities in Electoral Processes,” *Organization for Security and Co-operation in Europe*, 2014, www.osce.org/odihr/elections/124067?download=true.
8. Horwitz, Sari, Nakashima, Ellen and Gold, Matea. “DHS tells states about Russian hacking during 2016 election.” *The Washington Post*, September 22, 2017. www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.c86030dfa7e5.
9. “H.R.1562 - SAFE Act.” *Congess.gov*, March 16, 2017, www.congress.gov/bill/115th-congress/house-bill/1562/text.
10. Kinzinger, Adam. “Text - H.R.5181 - 114th Congress (2015-2016): Countering Foreign Propaganda and Disinformation Act of 2016.” *Congress.gov*, May 10, 2016. https://www.congress.gov/bill/114th-congress/house-bill/5181/text.
11. Lee, Timothy. “DNC email leaks, explained.” *Vox*, July 25, 2016, https://www.vox.com/2016/7/23/12261020/dnc-email-leaks-explained.
12. Mehrbani, Rudy. "States: Seize this Moment to Compel Congress’ Help in Shoring Up Voting Systems." *Brennan Center for Justice*. November 10, 2017. www.brennancenter.org/blog/states-seize-moment-compel-congress-help-shoring-voting-systems
13. Meko, Tim, Lu, Denise, and Gamio, Lazaro. “How Trump won the presidency with razor-thin margins in swing states,” *The Washington Post*, November 11, 2016. www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

14. "Minsk Declaration and Resolutions." *Organization for Security and Cooperation in Europe*. July 9, 2017. ccdcoe.org/sites/default/files/documents/OSCE-170709-MinskDeclaration.pdf.

15. "National Security Imperative of Addressing Foreign Cyber Interference in U.S. Elections." *Brookings*, August 29, 2017. www.brookings.edu/events/national-security-imperative-of-addressing-foreign-cyber-interference-in-u-s-elections/.

16. Norden, Lawrence and Famighetti, Christopher. "America's Voting Machines at Risk." *Brennan Center for Justice*, September 15, 2015. www.brennancenter.org/publication/americas-voting-machines-risk.

17. Schleifer, Theodore and Walsh, Deirdre. "McCain: Russian Cyberintrusions an 'Act of War.'" CNN. Accessed October 5, 2017. www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html.

18. Schlesinger, Robert. "Hack the Vote: a reminder of how insecure our ballots can be." *U.S. News & World Report*, July 31, 2017. www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are.

19. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." *Department of Homeland Security*, Jan 6, 2017. www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

20. "Tallinn Manual on the International Law Applicable to Cyber Warfare." *Cambridge University Press*, 2013. www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

21. Van der Meer, Sico. "EU Creates a Diplomatic Toolbox to Deter Cyberattacks." *The Council on Foreign Relations*. June 20, 2017. www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks.

22. Von Spakovsky, Hans A. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' *The Heritage Foundation*, August. 17, 2016. www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure.

23. "Written Testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Intelligence Hearing Titled "Russian Interference in the | Homeland Security." Accessed October 6, 2017. www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

The OSET Institute and TrustTheVote Project are supported by grant making organizations, philanthropists, and individual supporters like you. Financial support of the OSET Institute is tax-deductible (Fed. Tax ID: 20-8743186).

Over a decade of dedication to improving election technology integrity

530 Lytton Avenue
2nd Floor
Palo Alto, California 94301 USA
650.600.1450
www.osetfoundation.org