OSET INSTITUTE

Briefing

Version 4.0

Cyberterrorist Threats to Election Technology Infrastructure

Commentary for Public-Policy Initiatives

Prepared for:
U.S. Election Administration Leadership

Prepared By:

Joy London
Associate General Counsel &
Director, International Development

With Contributions By:
Gregory A. Miller
Co-Founder

February 2019

Preface

In 2017, the U.S. intelligence community asserted that Russian government agents sought to undermine the American electorate's faith in its democratic process by performing covert cyber operations to exploit weaknesses in voter registration databases in as many as 39 states.[1] Russia and the U.S. — or any sovereign nation, for that matter — should support the notion of self-determination — a country's right to structure their own government as it sees fit,[2] including the freedom to hold elections without extraterritorial influence, coercion or manipulation.

The Russian government's cyber operations during the 2016 U.S. election brought to the forefront the idea of "cyberterrorism," a bandied-about term with no clearly agreed-to definition. Acts of cyberterrorism could be directed against this country's election infrastructure, now designated as one of the 16 vitally important economic and civic sectors that make up the nation's "critical infrastructure." In fact, at least two bills, H.R.1 and H.R.52, have been introduced in the new 116th Congress, as well as several recently published, stand-alone national strategies that brings into finer focus, the issue of potential cyberterrorist threats to America's election infrastructure.

[1] https://www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions

[2] https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3696&context=bclr

Background

An interesting potential public policy development has surfaced given the arrival of H.R. 1 and H.R. 52.

On January 3, 2019, the first day of the 116th session of Congress, Rep. John Sarbanes [3](D-MD-3), the Chair of the Democracy Reform Task Force,[4] introduced the much-publicized House Resolution #1 (H.R.1 - For the People Act of 2019[5]), a 571-page bold reform bill package to restore the promise of our democracy — a government of the people, by the people, for the people. The bill proposes a national strategy to protect voters' rights, end gerrymandering, enhance election integrity, remove dark money political spending, and boost election security. But H.R.1 contemplates a far less publicized national strategy — protecting critical democracy infrastructure[6] ("CDI") as a matter of national security.

Section 3201(b)(1) of H.R.1 reads:

> *The national strategy required under subsection (a) shall include consideration of the following: (1) The threat of a foreign state actor, foreign terrorist organization (as designated pursuant to section 219 of the Immigration and Nationality Act 10 (8 U.S.C. 1189[7]), or a domestic actor carrying out a cyber-attack, influence operation, disinformation campaign, or other activity aimed at undermining the security and integrity of United States democratic institutions.*

Pay close attention to section (1) in this excerpt. Here is the interesting development: On the same day H.R.1 was introduced by Sarbanes, Rep. Sheila Jackson Lee [8](D-TX-18) reintroduced one of her bills[9] from the last session of Congress — H.R.950 – SAFETI Act,[10] the Security for the Administration of Federal Election from Terrorists Intervention Act of 2017. The 2019 version of the bill (H.R.52[11]) is exactly the same as the 2017 version.

Section 2 of H.R.52 reads:

> *Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Comptroller General of the United States and Congress a report on actions taken by the Department of Homeland Security relating to terrorist threats[12] to the integrity of elections for Federal office held in 2016.*

[3] https://www.congress.gov/member/john-sarbanes/S001168

[4] https://democracyreform-sarbanes.house.gov/

[5] https://www.congress.gov/bill/116th-congress/house-bill/1

[6] http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure

[7] https://www.law.cornell.edu/uscode/text/8/1189

[8] https://www.congress.gov/member/sheila-jackson-lee/J000032

[9] https://homelandprepnews.com/stories/32047-rep-jackson-lee-reintroduces-homeland-security-bills/

[10] https://www.congress.gov/bill/115th-congress/house-bill/950/

[11] https://www.congress.gov/bill/116th-congress/house-bill/52

[12] https://www.congress.gov/bill/116th-congress/house-bill/52/text

However, as worded, H.R.52 seems to suggest that the Department of Homeland Security might have information about *terrorist threats* to the integrity of the 2016 elections for Federal office. Or perhaps, the bill can be read to elevate kinetic attacks or cyber-attacks on election systems to the urgency of threats posed by notorious foreign terrorist organizations like Al-Qaeda, ISIS and others known for their terrorist attacks worldwide. So how *should* we think about non-state attacks on our election infrastructure[13] by terrorists, rogue states, and criminal networks.

Per my conversation with Lillie Coney, Policy Director for Rep. Jackson Lee, H.R.52 is an effort to address prospective cyber-terrorist attacks on voting systems in federal elections in 2020 and beyond. Yet, given Congresswoman Jackson Lee's important roles on the Homeland Security committees — the Subcommittee on Cybersecurity and Infrastructure Protection[14] and the Subcommittee on Counterterrorism and Intelligence[15] — one cannot help but wonder what these subcommittee members may know — and/or what they may anticipate in future federal elections.

What would a cyber-terrorist attack against our election infrastructure look like?

Cyber-terrorism — Defined

Dorothy Denning,[16] a noted computer scientist and professor at the Naval Postgraduate School, offers the best operational definition of cyberterrorism:[17]

> *Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*

According to Denning's definition of cyber-terrorism, would a cyber-attack on the components of our election systems — now designated "critical infrastructure"[18] — be considered an act of cyber-terrorism? Or, alternatively, are elections and voting systems "nonessential services?"[19] Since its beginning, the OSET Institute has made arguments that an election system, at least when in operation (as differentiated from a "stored" or "dormant" state), is indisputably

[13] https://www.dhs.gov/topic/election-security

[14] https://homeland.house.gov/subcommittees/cybersecurity-and-infrastructure-protection-116th-congress

[15] https://homeland.house.gov/subcommittees/counterterrorism-and-intelligence-116th-congress

[16] http://faculty.nps.edu/vitae/cgi-bin/vita.cgi?id=1074712524&p=display_vita

[17] https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[18] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[19] https://www.law.cornell.edu/uscode/text/42/5189e

essential in service to the sovereign act of holding free, fair and trustworthy elections, and to the operational continuity of American democracy. Given that the Twentieth Amendment of the Constitution requires the president-elect to take the oath of office at noon on January 20 following a federal election, coupled with the objective of an election infrastructure attack — i.e., to call election results into question, or to sow distrust in our system generally — then it can be argued that any attempt to derail a national election (let alone a successful attempt) is an attempt to sow seeds of terror.

It's worth noting the Merriam-Webster definition[20] of "terror" is "*a state of intense fear; a frightening aspect; a cause of anxiety; worry…*" One "frightening aspect" or "cause of anxiety" here would be civil unrest in response to an uncertain outcome in a Presidential election. Such anxieties only intensify when a date certain bears down upon election officials to certify the results of elections before a peaceful and the orderly transfer of power. (There are, essentially, no do-overs; no "mulligans."[21])

To put a fine point on it, the U.S. Code of Federal Regulations defines "terrorism" as

> *"[t]he unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85(l)[22])"*

Critical Infrastructure — Defined

Note that, for purposes of defining "critical infrastructure," the OSET Institute does *not* consider the Internet, per se, to be a component of election systems. Certainly, the Internet figures in making available election administration services — like, say, electricity — though I make this distinction from the *actual act of voting*.

The definitions above will suffice to identify "terrorism" in the exploitation of the open public Internet for electioneering and manipulating campaigns. However, the mere attempt at a propaganda, disinformation, or influence operation (what the OSET Institute refers to as a Type-I defamation attack) is quite different from an effort to actually disrupt or subvert the process of voting (a Type-II disruption attack or a Type-III subversion attack).[23]

These latter two types of attacks share an interesting membrane when a Type-I attack is focused not on an issue or political candidate, but on the election administration process itself, or its related equipment, as the OSET Institute sees, for example, when the English language is used to place elections in the realm of pseudo-warfare with words like *hacked*, *rigged*, and *tampered*.

[20] https://www.merriam-webster.com/dictionary/terror

[21] https://www.merriam-webster.com/dictionary/mulligan

[22] https://www.law.cornell.edu/cfr/text/28/0.85

[23] http://www.osetfoundation.org/blog/2018/9/19/will-foreign-adversaries-attack-in-us-midterm-elections-or-elsewhere

Cyberterrorism — Addressing a National Strategy

Thus, a compelling argument can be made that cyberterrorists pose a threat to elections, and "cyberterrorism" may be a broader way to describe election cyber-attacks. Nevertheless, I acknowledge this position is debatable. For guidance on this issue, I turn to recent national cyber strategies released by the Office of the White House.

In September 2018, the White House issued the National Cyber Strategy of the United States of America.[24] This cyber strategy includes the following language:

> *State and local government officials own and operate diverse election infrastructure within the United States. Therefore, when requested we will provide technical and risk management services, support training and exercising, maintain situational awareness of threats to this sector, and improve the sharing of threat intelligence with those officials to better prepare and protect the election infrastructure. The Federal Government will continue to coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system. In the event of a significant cyber incident, the Federal Government is poised to provide threat and asset response to recover election infrastructure.*

One month after the publication of this National Cyber Strategy, President Donald Trump released a National Strategy for Cyberterrorism.[25] Sections of this strategy include the following:

> *Critical infrastructure has long been subject to physical threats and is now increasingly exposed to the risk of attacks in cyberspace.*
>
> *We will also ensure that America's critical infrastructure is protected, in order to deter and prevent attacks, and is resilient so that we can quickly recover should it come under attack.*
>
> *We will also deploy new technologies precisely where they are needed and protect critical infrastructure in the United States from terrorist attacks.*

A combined reading of these two national strategies might help lawmakers focus their attention on securing election "critical infrastructure" through the lens of cyber-terrorists. Other countries, such as Ukraine, have done just that.

Days before the 2014 presidential elections in Ukraine, a pro-Russian hacktivist group claimed responsibility for shutting down Ukraine's Central Election Commission's computer systems. With another upcoming presidential election in 2019, leaders in Ukraine are concerned about combatting another cyber-terrorist attack.

[24] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[25] https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf

The Ukrainian Election Task Force[26] (established by the Atlantic Council,[27] the Victor Pinchuk Foundation,[28] and the Transatlantic Commission on Election Integrity[29]) recently published a brief predicting:

> *Moscow is expected to use kinetic means to influence Ukraine's March, 2019 election by . . . continuing and increasing acts of sabotage and terrorism, such as . . . attacks on . . . and interference against critical civilian infrastructure . . .*[30]

The U.S. Congress has taken a keen interest to protect Ukraine's critical infrastructure against cyber-attackers who seek to undermine that country's democracy. In the last session of Congress both the House and the Senate introduced companion bills H.R.1997[31] and S.2455[32] – the Ukraine Cybersecurity Cooperation Act to "*provide Ukraine such support as may be necessary to secure government computer networks from malicious cyber intrusions, particularly such networks that defend the critical infrastructure of Ukraine.*" [Section 4(a)(1)]

Meanwhile, in April, 2018, Ted Piccone,[33] a senior fellow at The Brookings Institution, stated:

> *Non-state actors from the radical right and the left, and those engaged in terrorism,*[34] *are also exploiting the open nature of the Internet for multiple purposes, including influencing public opinion before and during elections.*

Notwithstanding the discussion above, public policy considerations, thus far, have focused on deterrence of cyber-terrorism in specific sectors of U.S. critical infrastructure (e.g., dams, energy, nuclear reactors, transportation systems, water and wastewater systems, etc.). Little attention, to date, has been paid to "*terrorist threats*" on election technology infrastructure, as opposed to "terrorist threats" occurring close to an election or on Election Day.

One message remains clear: Congress has a lot of work to do, beyond H.R.1 and H.R. 52, to protect our elections and election infrastructure in time for 2020 and beyond.

[26] https://www.atlanticcouncil.org/images/publications/Ukrainian-Election-Task-Force-Exposing-Interference-in-Ukraines-Democracy1.pdf

[27] https://www.atlanticcouncil.org/

[28] https://pinchukfund.org/en/

[29] http://www.allianceofdemocracies.org/initiatives/the-campaign/press_release_tcei/

[30] https://www.atlanticcouncil.org/images/publications/Ukrainian-Election-Task-Force-Exposing-Interference-in-Ukraines-Democracy1.pdf

[31] https://www.congress.gov/bill/115th-congress/house-bill/1997

[32] https://www.congress.gov/bill/115th-congress/senate-bill/2455

[33] https://www.brookings.edu/experts/ted-piccone/

[34] http://sur.conectas.org/en/democracy-and-digital-technology/

For Further Reading

- National Intelligence Strategy of the United States of America — 2019
  https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
- Elections and the Timing of Terrorist Attacks
  https://www.jstor.org/stable/10.1017/s0022381614000504
- Executive Branch Power to Postpone Elections
  https://fas.org/sgp/crs/RL32471.pdf
- Transforming Election Cybersecurity
  https://www.cfr.org/report/transforming-election-cybersecurity
- Why Do Terrorists Love to Strike Around Elections?
  https://www.brookings.edu/opinions/why-do-terrorists-love-to-strike-around-elections/

About the Author

Joy London is the Associate General Counsel and Director of International Development at the **OSET Institute**, where her work focuses on critical democracy infrastructure, election law, public policy and international government relations. Ms. London earned her JD from Temple University School of Law and is licensed to practice law in the State of New York. Joy has held several positions at international law firms, and most recently, worked at one of the Big-4 management consulting firms. She earned a Master of Professional Studies in Cyber Policy & Risk Analysis from Utica College, and published a Capstone research paper: *The Threat of Nation-State Hacking of State Voter Registration Databases in U.S. Presidential Elections*.

Mail: jlondon@osetfoundation.org