COUNCIL *on* FOREIGN RELATIONS

CYBER BRIEF

Transforming Election Cybersecurity

David P. Fidler
May 2017

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The 2016 U.S. election constituted a watershed for democracies in the digital age. During the election cycle, fears proliferated among policymakers and the public that foreign actors could exploit cyber technologies [PDF] to tamper with voter registration, access voting machines, manipulate storage and transmission of results, and influence election outcomes. Russian information operations and disinformation on social media compounded these fears about election cybersecurity by raising questions about foreign interference with the election's integrity. Similar worries have arisen with elections this year in France, Britain, and Germany, and the Netherlands opted to hand count ballots in its March election to prevent hacking from affecting the outcome. In May 3 testimony to the Senate Judiciary Committee, James B. Comey, former director of the Federal Bureau of Investigation, indicated that Russia had tried to tamper with vote counts in other countries and that it might attempt to do the same in the United States in the future.

Technical strategies [PDF] to protect election systems from cyber interference exist, such as stopping the use of voting machines connected by wireless networks and deploying machines that produce auditable paper trails. However, the events of 2016 demonstrate that more high-level political action is required to manage real and perceived cyber vulnerabilities in election systems. Government officials and nongovernmental organizations that support elections should adopt measures to protect election systems from online threats, deter cyber interference with such systems, and reassure citizens their right to vote is defended. Achieving these objectives requires local, national, and international actions to strengthen cybersecurity in election systems and to elevate election integrity in cybersecurity policies, human rights activities, and election assistance and monitoring.

BACKGROUND

Digital technologies and the internet have affected how elections are conducted, including through internet voting and online voter registration. Although reliance on computers and communication networks for elections has garnered some attention [PDF], election cybersecurity has not been politically prominent within democracies.

In the United States, the Constitution assigns responsibility [PDF] for elections to state governments. This "clunky" system means hackers have to breach numerous state and local electoral processes to achieve broad impact. After the "hanging chad" controversy of the 2000 election, Congress funded the adoption of electronic voting machines, which made computer, information, and network security critical to electoral integrity. The federal Election Assistance Commission (EAC) issued voluntary voting guidelines in 2005, which included security guidance for software, telecommunications, and wireless communications. However, in 2014, the Presidential Commission on Election Administration asserted [PDF] that the EAC's process of adopting guidelines "has broken down" because of "a lack of commissioners" and "disagreement over the agency's mission." This commission identified tensions between computer experts and election officials over the security of electronic voting technologies. Although cybersecurity risks grew significantly after 2005 in the public and private sectors, the EAC took a decade to update its guidelines [PDF] to address these and other risks to election security.

Interest in, and security concerns about, electronic voting have also arisen in other democracies. Some, such as Estonia and Switzerland, began using online voting, but others returned to paper ballots after trying electronic voting technologies. The Council of Europe made recommendations for electronically enabled elections in 2004 and began updating them in 2015 to address technological developments, including new cybersecurity risks.

However, cybersecurity policies over the last decade have reflected little interest in elections. To date, most democracies have not specifically criminalized cyber interference with election systems. Policy on cyber terrorism focuses on threats to critical infrastructure, but it appears no government designated election systems critical infrastructure until the United States in January 2017. Studies of cyber espionage and cyber warfare have not highlighted election cybersecurity. Cybersecurity efforts in U.S. states are uneven in effectiveness, and pre-2016 analysis of state-level policies [PDF] rarely focused on elections.

CHALLENGES FOR ELECTION CYBERSECURITY

In the United States, the constitutional assignment of election management to the states raises federalism problems for improving election cybersecurity. For example, state election officials [PDF], some members of Congress [PDF], and an EAC commissioner opposed the federal government's designation of election systems as critical infrastructure. Additionally, the EAC has often lacked sufficient commissioners to function effectively, and proposed legislation seeks to terminate it. After the 2000 election, the federal government provided funds to help states modernize election systems, but when that funding ended, states often did not devote resources to improve and sustain updated systems.

Internationally, many democracies [PDF] are concerned about cyber threats to election systems. However, nationalist and populist movements have preoccupied the United States and European democracies with domestic problems and difficult relations over trade, defense and security issues, and Russia.

Generating U.S. leadership on election cybersecurity will be a challenge because the Donald J. Trump administration is unlikely to prioritize it. Without evidence, President Trump has attacked the U.S. election system as "rigged" by elites and riddled with domestic fraud, and he shows no willingness to confront Russia over its influence operations during the 2016 U.S. election or the 2017 elections in European democracies. This state of affairs requires actions at home and abroad not dependent on White House leadership.

RECOMMENDATIONS

A comprehensive strategy should heighten the political attention cybersecurity receives in efforts to ensure the integrity of elections; it should also make election integrity a more important part of cybersecurity policy.

At the state level, governors can make election cybersecurity a priority by supporting the election cybersecurity task force created by the National Association of Secretaries of State and turning the election aspects of the 2016–2017 Meet the Threat cybersecurity initiative of the National Governors Association (NGA) into a permanent component of the NGA's activities. States' attorneys general can raise the political profile of election cybersecurity by tackling it in the National Association of Attorneys General's special committee on internet safety/cyber privacy and security.

At the federal level, the designation of election systems as critical infrastructure should remain. The designation ensures election systems receive priority cybersecurity assistance from the Department of Homeland Security (DHS). The designation does not threaten federalism, and it facilitates information sharing and technical assistance. DHS, supported by the National Institute of Standards and Technology, should take responsibility for issuing guidelines on election cybersecurity. Additionally, the Department of State should expand the U.S. intelligence community's information sharing with European countries on election cyber threats into a multi-democracy initiative on election cybersecurity, perhaps through the Global Forum on Cyber Expertise or by partnering with the International Institute for Democracy and Electoral Assistance.

At the international level, intergovernmental and nongovernmental bodies that monitor elections and provide assistance to electoral systems should craft harmonized international principles on the use of electronic voting technologies. These principles should address, among other things, election cybersecurity and should draw on recommendations from governments, international institutions, and nongovernmental organizations. The National Democratic Institute (NDI) has identified common features of existing recommendations, including on election system cybersecurity.

A model for developing harmonized principles is the NDI's collaboration with the UN Electoral Assistance Division on the principles for international election observation [PDF]. Under this model, election observation mechanisms, such as those operated by the Organization of Security and Cooperation in Europe and the Organization of American States, should participate. Similarly, nongovernmental leaders in election observation and assistance, such as the Carter Center and the International Forum for Electoral Systems, should contribute to developing the harmonized principles.

Such layered state, federal, and international actions would deter cyberattacks on election systems by making such attacks more difficult, costly, and ineffective. Furthermore, democracies should add specific offenses for interfering with election systems to domestic cybercrime laws and the Council of Europe's Convention on Cybercrime. Criminal law should support the prosecution of hacking of election systems as it does cybercrime, cyber espionage, and economic cyber espionage.

Democratic countries that have not already done so should declare that their election systems are critical infrastructure and that international law and cyber norms protecting critical infrastructure apply to such systems. Democracies should articulate that cyber interference with election systems violates the international legal principles of sovereignty and nonintervention; they should also identify diplomatic, trade, travel, and financial countermeasures, such as economic sanctions [PDF], that they will impose against state actors responsible for such interference.

In addition, democracies should emphasize election cybersecurity's importance in protecting the human right to vote in free and fair elections. European democracies should pursue this goal in the European Union and Council of Europe and seek action in the UN human rights system, such as updating the authoritative guidance on voting rights issued in 1996 to address, among other things, election cybersecurity.

Allegations of, and fears about, cyber meddling in election systems undermine confidence in the democratic process and threaten citizens' trust in voting. Protection and deterrence are necessary, but reassuring voters of the importance and effectiveness of election cybersecurity policies is also critical. The threats of foreign information operations and disinformation spreading through social media during elections make reassurance on election cybersecurity even more important.

First, government officials and nongovernmental organizations should identify the cyber threats election systems face before election cycles. Information about these threats would provide citizens with facts and guidance that can help make them less susceptible to rumors, disinformation, and sensationalist fears that are spread on social media. Second, government officials responsible for administering elections should demonstrate they can defend election systems from cyber threats through, among other things, explaining protective actions, testing defensive measures, and participating in oversight processes. Third, as election cycles unfold, officials should make clear to the media and the public how they are protecting election systems from cyber interference. Reassurance should include postelection reviews and revision of election cybersecurity strategies as needed.

Protection, deterrence, and reassurance measures will strengthen election cybersecurity and can support calls to upgrade outdated voting machines [PDF] and identify the next generation of voting technologies. Internet freedom is in trouble, and cyber-subversion threats to democratic elections also include operations against candidates, political parties, and the dissemination of fake news. Efforts to address these problems are underway, including the Protect Your Election initiative for journalists and news organizations and strategies to combat disinformation on social media. Similarly, democracies should not allow cyber threats to election systems—real or perceived—to undermine the role voting plays in democratic sovereignty and individual liberty. Fortunately, election cybersecurity is within reach everywhere citizens cast votes.

About the Author

David P. Fidler is adjunct senior fellow for cybersecurity at the Council on Foreign Relations, the James Louis Calamaras professor of law at Indiana University's Maurer School of Law, and an associate fellow with the Centre on Global Health Security at Chatham House. He is an expert in international law, cybersecurity, national security, counterinsurgency, biosecurity, and global health. Fidler's publications include *The Snowden Reader* (editor and contributor), *India and Counterinsurgency: Lessons Learned* (coeditor and contributor), *Responding to National Security Letters: A Practical Guide for Legal Counsel* (coauthor), *Biosecurity in the Global Age: Biological Weapons, Public Health, and the Rule of Law* (coauthor), and *SARS, Governance, and the Globalization of Disease* (author). He holds a BCL from the University of Oxford, a JD from Harvard Law School, an MPhil in international relations from the University of Oxford, and a BA from the University of Kansas, and he was a Truman scholar from Kansas.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program aims to identify solutions to one of the world's most pressing challenges in the twenty-first century: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program produces research and analysis on the politics of cyberspace. Cyber Briefs are short memos that provide concrete recommendations on topics related to online privacy, cybersecurity, Internet governance, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.