Russia Today, Cyberterrorists Tomorrow: U.S. Failure to Prepare Democracy for Cyberspace

Jonathan F. Lancelot
Norwich University, Jonlancelot@me.com

Follow this and additional works at: https://commons.erau.edu/jdfsl

Part of the Computer Law Commons, Databases and Information Systems Commons, Election Law Commons, Information Security Commons, International Relations Commons, Software Engineering Commons, and the Systems Architecture Commons

Recommended Citation
DOI: https://doi.org/10.15394/jdfsl.2018.1533
Available at: https://commons.erau.edu/jdfsl/vol13/iss4/6

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.
RUSSIA TODAY, CYBERTERRORISTS TOMORROW: U.S. FAILURE TO PREPARE DEMOCRACY FOR CYBERSPACE

Jonathan F. Lancelot
Norwich University

ABSTRACT

This paper is designed to expose vulnerabilities within the US electoral system, the use of cyberspace to exploit weaknesses within the information assurance strategies of the democratic and republican party organizations, and deficiencies within the social media communications and voting machine exploits. A brief history of discriminatory practices in voting rights and voting access will be set as the foundation for the argument that the system is vulnerable in the cyber age, and the need for reform at the local, state and national levels will be emphasized. The possibility of a foreign nation-state influencing the outcome of an election by using cyber warfare tactics should give us pause as this opens the US democracy to terrorist organizations who have the means to disrupt a US election via cyber-attack.

Governments keep their promises only when they are forced, or when it is to their advantage to do so.  -Napoleon Bonaparte

1. THE ROOTS OF A VULNERABLE DEMOCRACY

If we want to get to the root of the problem of US elections being influenced by forces other than the winds of democracy and the will of the American people, we must look to the history of disenfranchisement and the exclusion of specific groups of Americans from voting or having a stronger voice within the public dialog. For example, “throughout the history of our country, those in power have devised a multitude of devices to diminish voting power. These include gerrymandered voting districts, all-white primary elections, literacy tests, poll taxes, arcane voter registration procedures, and annexation of white suburban neighborhoods by cities about to achieve a black voting majority” (The JBHE Foundation, Inc, page. 61). This is a reality of US history that still haunts the US electoral system since the passage of the Voting Rights Act of 1965. There are remnants of the government’s past in disenfranchisement that continue to eat at the social fabric and the democracy itself. “The personal cost of voting is a potentially important part of the decision calculus as well. Recent voter-ID laws potentially increase this cost in at least two ways. First, voters who fail to supply the necessary identification may be turned away without voting. Second, there are sometimes monetary and preparation costs associated with voter-ID laws that voters must incur. These costs may be relatively low or high depending on a voter’s level of sophistication, work flexibility, or income” (Mycoff, Wagner, Wilson, page. 121). Third, the sunsetting of important clauses within the Voting Rights Act has allowed states to return
to behavior that excluded certain voters and continue to create room for fraud and new vulnerabilities before we even explore the cyber element of US elections. “Representative John Lewis—an icon of the civil-rights struggle—highlighted remaining challenges to equitable voting and called for continued work on rights” (Graham, page. 4), and the fact that the problem of rights is still an issue the US government is struggling to demonstrate the potential for an electoral disaster that will be even worse than a rival nation-state interfering in US elections.

The US Electoral System struggles with corruption within the dealings of politicians (of both major political parties), lobbyists and donors. For instance, criminal behavior around voting machines has placed doubt on the integrity of election results. “Rep. Vernon Ehlers (R-Mich.) lays most of the blame for current electronic voting machine failures with former Rep. Bob Ney (R-Ohio), who preceded Ehlers as House Administration chairman who was sentenced in connection to his association with disgraced lobbyist Jack Abramoff” (Murray, page. 2). It also does not help to secure a democratic system when unlimited monetary funds can be dumped into a candidate’s campaign to give them an unfair advantage or can be dumped into an election cycle to influence the results on election day. “In Citizens United v. FEC, the Supreme Court again addressed a First Amendment challenge to the ban on corporate electioneering activities. After two rounds of brief and oral arguments, a narrow majority of the Court overturned Austin v. Michigan State Chamber of Commerce and portions of McConnell v. FEC and struck down the portions of the Bipartisan Campaign Reform Act of 2002 that prohibited expenditures on electioneering communications by corporations” (The Harvard Law Review Association, page. 76). The roots of vulnerability within the US election system are broad, and election interference (in the democratic process) is not a new problem. What is new is the ability of rival nation-states and terrorist organizations to utilize cybercrime, cyber espionage, and cyber warfare to disrupt the democratic process, endangering the citizenry.

2. DEEP ROOT ANALYTICS: GIVING AWAY THE SHOP

Information gathering on voter attitudes and preferences is nothing new in American politics. Democratic and Republican parties are both patrons of companies like Deep Root Analytics that give them an edge in predicting voter behavior and tethering their strategies to such information. Unfortunately, “the firm left 198 million voter records unsecured online for nearly two weeks. This should give every American pause, particularly at a time when intelligence officials say the Russian government actively seeks to undermine American elections” (Lapawsky, page. 2). The data theft was significant, and the amount of data stolen is staggering. “This particular breach, discovered by researcher Chris Vickery, exposed 1.1 terabytes of personal information compiled by Deep Roots Analytics, a company that analyzes not just basic data like names and addresses, but also scores how particular voters feel about a range of political issues, from gun control to offshoring in the auto industry. Vickery’s discovery illustrates how poorly organizations safeguard sensitive information” (Lapawsky, page. 2). As every aspect of a person and organizations life is in cyberspace, democratic institutions are no different. Secure US elections as they are structured today provides no security and integrity to the vote and provide no cybersecurity or information assurance. Questionable data collection does not always have to be from a breach; the controversy
between Facebook and Cambridge Analytica is an instance where a social media company seemed to hand over customer data over a private data collecting organization, which made efficient use of the information towards a political end. “Cambridge Analytica, a political data firm fired by President Trump’s 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior” (Granville, New York Times). In this case, Facebook was allegedly complicit in the scheme. How much the company at the highest levels knew, and when they knew it does not even matter at this point, Facebook is currently receiving devastating criticism from governments internationally for their lack of oversight in customer privacy. In the United Kingdom (UK), “the Digital, Culture, Media, and Sports (DCMS) Select Committee’s far-reaching interim report on its 18-month investigation into fake news and the use of data and ‘dark ads’ in elections offer a wide-ranging, informed and sustained critique that with it the full weight of parliament. The verdict is withering: Facebook failed” (Cadwalladr, The Guardian). The failure is rooted in the social media company’s recalcitrance in mitigating the unauthorized release of customer data, deliberate or not. In concurrence, the fact that a political campaign hired Cambridge Analytica leads to the issue of domestic abuses of elections which is an issue embedded within the history of US political culture.

The fact that US politicians have influenced elections domestically using illegal methods is well known. However, the implications of US politicians influencing elections with the aid of a foreign nation-state or foreign entity is disastrous. “Suspicion has mounted about whether the Trump campaign somehow colluded with Russian actors to influence American voters” (Lapawsky, page 2). This matter is still under investigation. The 2016 election was rife with elements of cybercrime, and the case of the DNC hacking incident is most intriguing, as the cybercrime of hacking into DNC servers exposed domestic instances of anti-democratic practices within the Democratic primary. “The Kremlin has denied Russian involvement in the DNC breach. But the reverberations continued; DNC Chairwoman Debbie Wasserman Schultz resigned after emails revealed what many views as the unfair treatment of Bernie Sanders” (Glaser, Page. 4). The damage to the DNC organization was devastating, and the events of 2016 revealed that cyberwarfare is a reality as there is no guarantee the US government will be able to react to the next attempt on an election in the future. The democratic and republican organizations in the US Congress have shown no signs of coming together to solve the issue of cybersecurity and democracy and continue the behavior of hyper-partisanship which is a continuation of widening the fissures that makes future cyber-attacks on our elections more likely. “All is it amounts to a political system that needs to devote at least as much energy into securing its systems as it does into securing votes. At this point, there is no saying they weren’t warned” (Lapawsky, page 6), and it seems today the warnings has caused some panicking within the beltway.

3. CAN TERRORIST ORGANIZATIONS THWART THE DEMOCRATIC PROCESS?

In cyberspace, a non-state organization can do as much damage as an organization or a nation-state, and it could be done anonymously. Therefore, it is logical to
conclude that if Russia can allegedly do it, so can a sophisticated terror organization. For instance, “on February 16th, 2018 Special Counsel Robert S. Mueller III indicted 13 Russian individuals and three Russian organizations for engaging in operations to interfere with US political and electoral processes, including the 2016 presidential election. This was a significant step forward in exposing a surreptitious social media campaign and holding account those responsible for this attack” (US House of Representatives). The importance of looking at this issue beyond nation-state borders, as nation-states can either accept or deny responsibility is critical. In this case, the Russian government denies responsibility. “Russian Foreign Minister Sergei Lavrov came away from the meeting saying Trump had heard out Putin’s assurances that Moscow did not run a hacking and disinformation effort and had dismissed the entire US investigation into Russian role” (Filipov, Paletta, Phillip). Diplomatically, if we consider the Russian government was not involved with the hacking of the 2016 election, we should have pressed them to conduct their own investigation and give us their conclusion so both nation-states can narrow it down. If they refused, only then we would know conclusively if the Russian government was involved. Did the 13 Russian individuals and the three Russian organizations act as individuals? It is a reasonable question knowing the nature of the worldwide network, and the capability of acting anonymously or with a false identity. “Most hacking is motivated by nefarious and fraudulent aims.” (Hampson, page. 516). In fact, the Federal Bureau of Investigations (FBI) has calculated the financial cost to victims of cybercrimes outside the realm of political campaigns. In 2017, “the Internet Crime Complaint Center (IC3) says victims’ losses exceeded 1.4 Billion in 2017. Top ten crimes types reported to IC3 (by victim loss) are:

- Real Estate/Rentals, $56,231,333
- Investment, $96,844,144
- Advance Fee, $57,861,324
- Corporate Data Breach, $60,942,306
- Confidence Fraud/Romance, $211,382,989
- Identity Theft, $66,815,298
- Non-Payment/Non-Delivery, $141,110,441
- Personal Data Breach, $77,134,865
- Credit Card Fraud, $57,207,248
- Business E-Mail Compromise/E-Mail Account Compromise, $676,151,185” (FBI.gov).

So, we can conclude that well-funded terrorist and criminal organizations are capable of hacking elections, as long as they are supported by a nation-state’s resources and a strategic objective, for example organizing a massive DDoS attack on multiple candidate websites, or hack voter databases. Dan Wallach, a computer science professor at Rice University, notes that the internet is a ‘messy place’ with a lot of background traffic, and it would be difficult to find its origin because attackers are very good at hiding their location” (Sainz, page. 3). Therefore, the question is how do we verify a cyber-attack from a nation-state if government leaders deny responsibility? Most of all, how do we prevent democratic systems from being hijacked by rivals and terrorists?

4. POSSIBLE SOLUTION: E-GOVERNANCE

Lawmakers should consider legislation to protect the integrity of election results, election information, and democracy itself. “Officials bear a responsibility to our people and our Republic to embrace the best possible options,
and there are already opportunities to start. After election authorities learn of the advantages and scalability of blockchain voting, there is no excuse why they would continue to opt for only paper or only legacy electronic machines” (Spanos, page 2) unless they benefit somehow from the dysfunction and vulnerabilities within the system. Blockchain technology is one possibility of protecting voting and election results, yet there are noted issues and concerns with the innovation. “Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely difficult to change), and updateable only via consensus or agreement among peers" (Bashir, page. 16). Conversely, there are ways this innovative system can be hacked as well. First, "a Sybil Attack is an attack in which the same party owns a large number of nodes on a single network and attempt to disrupt network activity through flooding the network with bad transactions or manipulating the relaying of valid transactions" (Risberg). Second, “a routing attack is an attack made possible by the compromise or cooperation of an Internet Service Provider (ISP)” (Risberg). Third, “a Direct Denial of Service (DDoS) attack is an attempt by bad actors to cripple a server, anything from a website to a Bitcoin node, by flooding it with high volumes of traffic” (Risberg). Lastly, “The 51 percent or majority attack, since the security of a blockchain is directly linked to the computer power building the chain, there is the threat of an attacker gaining control over a majority of the hash power on the network" (Risberg). Blockchain technology is not a silver bullet and has vulnerabilities, yet some benefits need to be examined. For example, “Blockchain-secure voting machines work by allowing the voter to scan their own paper ballot, at which point the vote is simultaneously and immutably entered into the blockchain tally. A code is generated for the voter and observers, who are able to re-input the code to verify that the vote—with chain-of-custody proving the time and location—are forever entered into the result. This means that for the first time, elections are fully transparent and publicly auditable, down to each and every vote” (Spanos, page. 2). The US electoral system is federated and decentralized. Blockchain allows for a distributed software structure that would mirror the different features of each state’s electoral rules, increase the transparency and verify the integrity of every vote. “Centralized and distributed systems are architectural antipodes. Technical antipodes have always inspired engineers to create hybrid systems that inherit the strength of the parents” (Drescher, page.15). A blockchain voting system is a possible solution, or a partial solution to election fraud on most levels because of what the technology sets out to achieve. “The core problem to be solved by the blockchain is achieving and maintaining integrity in a purely distributed peer-to-peer system that consists of an unknown number of peers with unknown reliability and trustworthiness. This problem is not a new one” (Drescher, page.31). An example of a nation-state implementing blockchain is Estonia, “Its government is virtual, borderless, blockchained, and secure” (Heller). The country learned the hard way when their critical telecommunications infrastructure experienced a cyber-attack in 2007. Today, technology is linked throughout the society, and data is not collected in a centralized location and is protected by encryption at each node. "E-Estonia is the most ambitious project in technological statecraft today, for it includes all members of the government, and alters citizens' daily lives. The normal services that government is involved with—legislation, voting, education, justice, healthcare, banking, taxes, policing, and so on—have been digitally linked across one platform, wiring up the
nation" (Heller). In Estonia, it’s called e-
governance.

The structure of this system is arranged
where citizens can vote anywhere securely.
“Internet voting, or i-Voting, is a system that
allows voters to cast their ballots from any
internet-connected computer anywhere in the
world. Completely unrelated to the electronic
voting systems used elsewhere, which involved
costly and problematic machinery” (e-estonia).
Cybernetica, the company that developed i-
Voting states “the i-voting system consists of
Vote Forwarding Server, Vote Storing Server,
and Counter Server. They are responsible for
respectively collecting, storing and tabulating
i-votes. Counting Server is offline at all times
due to high-security requirements" (Cybernetica). The next level of the system is
“during a designated pre-voting period, the
voter logs onto the system using an ID-card or
Mobile-ID, and casts a ballot. The voter’s
identity is removed from the ballot before it
reaches the National Electoral Commission for
counting, thereby ensuring anonymity” (e-
estonia). The downside of blockchain voting
and remote voting is addressed as “with any
method of remote voting, including traditional
postal ballots, the possibility of votes being
forced or bought is a concern. Estonia’s
solution was to allow voters to log on and vote
as many times as they want during the pre-
voting period. Since each vote cancels the last,
a voter always has the option of changing his
or her vote later” (e-estonia). This is a possible
solution for our current electoral system,
voting, and governance. Innovation is key to
maintaining a stable democracy for the 21st
century, and tech companies like Cybernetica,
Nortal with verification services, and
OpenNodem, Ericsson, Telia, State
Infocommunication Foundation, and Dell EMC
for cloud services helped Estonia develop the e-
governance system. This is a model for the US
to aspire to and develop a system that is not
as open to exploit as it is today. Currently, the
US dealing with companies in charge of
holding sensitive voter data for political
campaigns getting hacked and using
technologies that have easily breached
vulnerabilities. For instance, “A political
robo-calling company called RoboCent exposed
4,500 client files to the open internet by failing
to properly configure its cloud storage on
Amazon Web Services” (Nordrum). This is a
devastating development that not only exposed
voter behavior to anyone willing to seek it out;
it endangers the very fiber of trust that is the
foundation of any true democracy. To solve
the issue of vulnerabilities that are created by
voter suppression, misinformation from
traditional and social media organizations,
political campaign hacking, legislatively
crippling partisanship, unlimited campaign
donations to candidates, and political parties’
officials rigging primary elections to the
advantage of their favored candidates, it must
be established that political cultures which
encourage vice and corruption is
counterintuitive to what a powerful
cybersecurity strategy can offer. "What is
often overlooked is the central role anti-
corruption, and human factors have to play in
countering this new technological menace"
(Black). The unifying and open nature of the
internet has also exposed and magnified the
deep flaws in the democratic process. It is a
contradiction for elected officials to state they
want to prevent interference, yet the constant
specter of corruption and illegal machination
remains as we continue into new election
cycles. "The leaders of four US intelligence
agencies reaffirmed at the White House on
Thursday that ‘pervasive’ and ‘ongoing’
threats from foreign actors, including Russia,
to interfere in upcoming US elections”
(Breuninger). Fortunately, “on January 6th,
2017, the Secretary of the Department of
Homeland Security (DHS) designated election
systems as critical infrastructure, created as a
subsector under the existing government security sector” (Homeland Security), yet this is not enough to protect our democracy and our national security. We need a unified government to agree on issues that address the vulnerabilities in our cyber-defense capabilities. Currently, there is no consensus on how to approach intermestic cyber policy and law enforcement issues. Nevertheless, the state of Utah used Cybernetica’s i-Vote technology “during 2016 Republican presidential caucus on the 22nd of March; voters had the opportunity to vote using the traditional methods or vote online” (Cybernetica). Consequently, there is no reason or excuse for the US government not to protect and defend the democratic institution enshrined by the Founders, and that is synonymous with protecting and defending the US Constitution. Today, waiting for the 9-11 of cyber-attack to react to a zero-day event takes us from a dangerous situation to a potentially crippling one. There needs to be a national conversation on the deep issues that divide and brings the people together, a conversation that will lead us to an upgraded method of governing our democracy. However, we are facing rivals that can shut down our elections with the push of a button, and time is running out.
REFERENCES


Russia Today, Cyberterrorists Tomorrow:...

www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic


