Interference with free and fair elections isn’t new. There have been a number of flawed elections in Latin America over the years. The U.S. doesn’t have clean hands in this discussion, either. Reportedly, the CIA bought elections for Christian Democrats in Italy (‘48) and Chile (‘64).

What is new in the 21st century is the use of cyberspace to facilitate manipulation of the democratic process. In Latin America, for example, actors with bad intentions have merely begun to use cyberspace as a method to control election results. There have been attempts to get inside various phases of the election process in the U.S., as discussed below. Most disturbing, there are large-scale manipulations of social media intended to undermine confidence in election results, or even change the outcome. The use of information to affect elections is discussed below, after a review of more traditional cyberspace methods that could be used against the electoral process.

There are a number of ways adversaries can exploit vulnerabilities in the election system. All of them contributed, to some extent, to casting a shadow over the 2016 presidential election.

The first is using cyber means to gain access to voter rolls. Online registration creates a fairly high vulnerability in the system. At least ten states had their registration systems hacked in the past cycle. In addition, there were at least twenty additional attempts. While it’s troubling to have this many attempts to access systems illegally, the attempts that are spotted probably represent the tip of the iceberg.

Accessing registration not only serves to introduce uncertainty in the system, it could also give hackers the opportunity to alter or delete voter files. That could mean that voters’ registrations wouldn’t appear to be valid when they attempt to vote, for example.

The cyber vulnerabilities that garnered the most attention during the presidential election were those involving voting machines. If hackers could gain access to the actual voting machines, votes could be changed, altering the outcome of the election. Such an attack could be nearly undiscoverable because, of course, voting is meant to be confidential so it’s challenging to design a system that would allow voters to ensure their votes were correctly counted, while protecting their vote from discovery by others.

Voting machines are designed to be secure, but every computer and cyber-based system has security shortfalls. Even air-gapped systems can be vulnerable. Vendors must update operating systems, which they often do with flash drives. Malware can be inadvertently or intentionally be introduced through the vector of a flash drive. Also, there must be some

---

2 http://www.bloomberg.com/feature/2016-how-to-hack-an-election/
3 https://www.thedailybeast.com/how-hackers-could-destroy-election-day/
7 http://www.thedailybeast.com/articles/2016/10/16/election-hackers-could-erase-you.html
Hacked Elections

way to load the ballots onto the machines, and that can be another method for hackers to penetrate systems.

Physically accessing machines to hack them is an exciting proposition, and it was sensationalized in the media. One expert said he could hack a given model of machine if he had seven minutes and a screwdriver.\(^8\) It may seem improbable that someone could hack a voting machine during an election, but voting machines are often stored in low-security locations, such as schools. It is possible they could be hacked while in storage.

In sum, there might be opportunities to hack voting machines, but payback on the investment for such a complex operation is likely low.\(^9\) One of the best defenses against machines being hacked is the fact that jurisdictions in the U.S. can’t agree on anything. There are at least six types and hundreds of models of voting machines in use across the U.S.\(^10\) Hackers would have to develop individual methods for penetrating a good number of them to have a significant effect. Further, unless the voting machines are connected to the internet, they must be penetrated individually or in relatively small groups that will allow malware to be passed from machine to machine. Some voting machines do have WiFi capability, but it is generally disabled as a defensive measure.

There are many ways to attack voting machines, but avoiding them doesn’t avoid the problem completely. The voting process can also face issues that don’t involve voting machines.\(^11\) For example, internet voting introduces new insecurity into the system. Thirty plus states already have internet voting in some form.\(^12\) This maneuver adds all the vulnerabilities of the internet to the mix. It opens up voting to attacks on individual elections. And, of course, the idea of slowing, disrupting, or taking down portions of the internet for periods of time, perhaps during an election, is now part of the cybersecurity conversation.\(^13\)

An unavoidable question when considering anti-election operations during the presidential election is, “Who is responsible?” For the most part, interference with the election has been attributed to Russia and an operation called Fancy Bear.\(^14\) Fancy Bear has also hacked election infrastructure in Ukraine,\(^15\) Poland, & Georgia, dissidents in France, plus sent

---


\(^10\) [https://www.verifiedvoting.org/resources/voting-equipment/] https://www.youtube.com/watch?v=bpMfM9qa570


\(^15\) [https://www.washingtonpost.com/opinions/russias-interference-in-ukraines-national-election-must-carry-consequences/2014/05/19/1e6487aa-df81-11e3-8dccc-d6b7fed081a_story.html?utm_term=.bc42d1bb127c](https://www.washingtonpost.com/opinions/russias-interference-in-ukraines-national-election-must-carry-consequences/2014/05/19/1e6487aa-df81-11e3-8dccc-d6b7fed081a_story.html?utm_term=.bc42d1bb127c)
Hacked Elections

communications that were allegedly from ISIS to France. The U.S. government has left no doubt as to who it believes is responsible.\(^\text{16}\)

Although domestic laws around the globe prohibit interfering with elections, there is little international law on the subject. If part of the attempt to affect the election is based on espionage or stealing information, that portion of the operation is unlikely to be actionable. All states engage in this type of operation for national security, and international law is silent on the subject.

An unusual aspect of the DNC case was that the perpetrators illegally took the information, but then released it publicly in an apparent attempt to manipulate public opinion. There is not much precedent for activity like this. Normally spying is not undertaken in order to release the information gained. Russia's attempts to manipulate the election apparently also used WikiLeaks as a proxy.\(^\text{17}\) To make activity like this more effective, information may be changed before its release. For example, DNC files may have been manipulated.\(^\text{18}\) However, there is dispute over this fact.\(^\text{19}\)

For lawyers, the question is whether cyber-based attempts to manipulate elections violate an international law or norm. Because espionage is not prohibited, we'd normally look to the prohibition on the use of force in Article 2(4) of the U.N. Charter, which bans international aggression.\(^\text{20}\) However, these operations don't cross the threshold of force as the term is normally defined.\(^\text{21}\)

The obligation of states to hold “genuine periodic elections” is enshrined in article 25 of the International Covenant on Civil and Political Rights (ICCPR), to which most states, including the U.S. and Russia are party.\(^\text{22}\) That provision was designed to ensure that states hold elections, not to preclude interference with the elections of other states. Interfering with external elections would violate the spirit of the ICCPR, but the agreement does not directly prohibit the activity.

Lacking more specific legal guidance, the relevant standard to determine if election interference activities are unlawful is whether the activity is a violation of sovereignty, perhaps a violation of the non-interference principle.\(^\text{23}\) In the case \textit{Military and}

\(^{19}\) http://dailycaller.com/2016/10/21/heres-cryptographic-proof-that-donna-brazile-is-wrong-wikileaks-emails-are-real/
Hacked Elections

Paramilitary Activities in and against Nicaragua Case (Nicaragua v. United States of America), the International Court of Justice (ICJ) noted that the principle of non-intervention involves “the right of every sovereign State to conduct its affairs without outside interference.” The ICJ concluded that the prohibition on interference is part of customary international law, which forbids states from “interven[ing] directly or indirectly in internal or external affairs of other States.”

Unfortunately, the ICJ did little to clarify exactly what kinds of activities would constitute wrongful interference. Scholars have weighed in on the issue, and generally there is a consensus that attempting to manipulate an election would violate the non-intervention norm. How, exactly, cyber enabled operations fit into that framework is still uncertain.

Looking back at the 2016 election, it has generally been concluded that there was no actual significant cyber interference with voting or vote counting. The government has discussed the vulnerabilities in the system and will, presumably, address them, although some of the fixes could introduce new vulnerabilities. The bigger problem is with the manipulation of the information surrounding elections, and this is a problem that will continue, especially when one state is far ahead of the rest of the world in the area.

Experts have concluded that Russia was responsible for the information campaign. Russia is skilled at using cyberspace to advance its national agenda and has leveraged disinformation on an industrial scale by, for example, spreading misleading claims about Sweden’s stockpiling of nuclear weapons, or stating that nuclear weapons on a Turkish base are at risk, and by persistently denying the presence of Russian troops in Ukraine. In addition, they have been comfortable allowing, even encouraging, private citizens to engage in offensive cyber activities when they coincide with national interests. This is in

25 Id.
27 For example, connecting machines to the internet could make them more vulnerable, and merely reducing the variety in machines would make it simpler for one attack to be designed that would affect all or most of the machines. Currently, the lack of consistency is a defense against hackers.
Hacked Elections

cast to the U.S. and other Western states, which generally do everything they can to prevent private actors from engaging in gray zone cyber activities.

Russia actively manipulates social media for its national security purposes, both internally and abroad. For example, people are hired to post negative comments about anti-Russia articles online, and do the opposite for pro-Russia articles, with the intent to overwhelm rational discourse on Western media sites. These Russian professionals have also used Twitter falsely to report an oil spill and an Ebola outbreak in the U.S., perhaps testing a capability to manipulate public opinion and create confusion and mistrust. Even if these false messages reach only a relatively small number of people, social networks have an extraordinary power to convince people and manipulate opinion by leveraging that small number in an ever-expanding ripple of disinformation.

The involvement of private entities in national cyber security is particularly important because corporations and other private groups can act in ways the government cannot, and act with information they already have in the course of business or from open sources. Many government activities would require accessing online information, yet proposals that make it easier—or even appear to make it easier—for the government to access private information are instantly condemned. The 2013 revelations of Edward Snowden caused a firestorm of protests against the NSA’s surveillance activities, even though the spying programs were lawful under U.S. law. The passing of the Cyber Intelligence Sharing and Protection Act (CISPA) in 2013 and Protecting Cyber Networks Act (PCNA) in 2015 also caused public outrage. There simply seems to be a consensus, at least among politically

36 CISPA directs the federal government to conduct cybersecurity activities to provide shared situational awareness enabling integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents. https://www.congress.gov/bill/113th-congress/house-bill/624.
37 This amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal governmental agencies, or state, tribal, or local governments; and (2) the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts. https://www.congress.gov/bill/114th-congress/house-bill/1560.
Hacked Elections

active citizens, that the government should not be allowed to access and monitor large quantities of citizens’ data, even to better ensure the security of the U.S.39

The resistance to the government being involved in the flow of private information, perhaps coupled with its ineffectiveness when it tries, has led to pressure on pressure on private companies to take steps to manage information online. This behavior by western corporations, motivated largely by business concerns, could be seen as the democratic equivalent of Russia’s operationalization of cyber criminals and hacktivists.

Google has a plan to fight fake news.40 Facebook and Twitter do, too, but none of the plans are without controversy.41

An illustration of how putting all this together can be challenging is Microsoft’s policy on dealing with “terrorist content.” Microsoft’s approach includes definitions of prohibited speech (which includes “…endorses a terrorist organization or its acts …”) and an exclusion for its search engine, which will still be allowed to return content responsive to searches for terrorist content.42 For the government to engage aggressively to remove content that is damaging to national security (i.e., terrorist recruiting, lethal knowledge like bomb making skills, or offensive propaganda) it must find a way to determine when unpleasant or undesirable speech crosses the line from constitutionally protected to legally impermissible, based on content or context. For the most part, corporations can avoid many of the constitutional issues that mire government efforts in the area, but still must contend with potential negative impacts to their bottom line from negative publicity.

The 2016 election is history, and democratic states need to draw lessons from it to secure their elections from outside cyber interference. Cyber attacks driven by technology, like in any internet-connected sector, will continue to be a challenge, but should be a manageable one. The truly vexing issue for democracies will be how to balance a respect for free speech and thought, while fending off manipulation of public opinion by states (or potentially other well-funded groups). The weaponization of information creates both legal and policy challenges that must be addressed.

40 https://qz.com/1195872/google-facebook-twitter-fake-news-chrome/.
42 Microsoft’s Approach to Terrorist Content Online (May 20, 2016), https://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000g8l17to0xdztzrca20pluw755v.