Dirty Tricks in the Digital Age

Cybersecurity and Election Interference

ELAINE C. KAMARCK

AND

DARRELL M. WEST

Dirty Tricks in the Digital Age: Cybersecurity and Election Interference
Elaine C. Karmack and Darrell M. West

How American elections are increasingly vulnerable—and what must be done to protect them

Until recently, most Americans could assume that elections, at all levels of government, were reasonably clean and well managed—most of the time. Yes, there were exceptions: some states and localities were notorious for occasional election-rigging, losers often complained that winners somehow had unfair advantages, and money increasingly distorted the electoral process. But even when voters did not like the results, the overall system of elections did not seem nearly as corrupt or warped as in many other countries.

That positive view of American politics now seems outdated, even naïve.

This new book by Elaine Kamarck and Darrell West shows how American elections have been compromised by what used to be called "dirty tricks" and how those tricks are becoming even more complex and dangerous the deeper we get into the digital age. It shows how old-fashioned vote-rigging at polling stations has been overtaken by much more sophisticated system-wide campaigns, from Russia's massive campaign to influence the 2016 presidential election through social media to influence campaigns yet to come.

Digital Dirty Tricks looks not just at the past but also toward the future, examining how American elections can be protected from abuse, both domestic and foreign. State governments have primary responsibility for elections in the United States, but the federal government also must play a major role in shaping the system for how Americans cast their votes.

The book explores what political leaders are doing and must do to protect elections—and how they can overcome the current toxic political climate to do so. It outlines five concrete steps that state and federal leaders must take to secure the future of American democracy.

Digital Dirty Tricks is a valuable resource for scholars, students, journalists, politicians, and voters—indeed, anyone interested in securing the most basic element of democracy.

Elaine C. Kamarck is a Senior Fellow in Governance Studies at the Brookings Institution. She directs the Center for Effective Public Management. She researches American politics and governance and is a member of the Democratic National Committee and worked in the White House in the 1990s.

Draft 9/4/19

Protecting Democracy: Cyber Security and Election Interference

By

Elaine C. Kamarck and Darrell M. West

Table of Contents

Introduction

You are sitting at home watching online videos and a friend sends you a link showing a seemingly real image of Senator Kamala Harris removing her clothes. She had recently done well in a television debate and was garnering widespread praise for her takedown of Democratic frontrunner Joe Biden. You watch with amazement. Is this for real? Would a United States Senator allow herself to be filmed doing that? How many people will see this? How is it going to affect the campaign?

Of course, the picture is not authentic. It is a "deepfake," something that no longer lies within the realm of science fiction or political fantasy. An AI developer named "Alberto" created grave consternation recently when he devised a "DeepNude" app that could "digitally undress women". The software "used artificial intelligence to create the 'deepfake' images, presenting realistic approximations of what a woman – it was not designed to work on men – might look like without her clothes."[i] The depictions were so realistic that they appeared genuine to many viewers. The backlash which ensued from his application was so strong that he took down the offering within a few days of starting to sell it for $50. In an interview, he explained he was able to create the tool by training it on 10,000 pictures of naked women. However, other developers have replicated the software so the world is not safe from DeepNude knockoffs.[ii]

This and other types of inventions show how far technology has come and what the political, ethical, and societal risks are as we head into Campaign 2020. Through current software, it is possible to develop and distribute content that is offensive and abusive. Editing tools are widely available to virtually anyone with access to a computer. Public skepticism about journalists means it likely will be difficult for news fact-checkers and gatekeepers to act as a counterweight to digital disinformation, doctored images, divisive rhetoric, and outright falsehoods. As took place in 2016, automated bots can distribute such materials widely and potentially affect the election outcome.

All of this is taking place in a country that is quite polarized; where there is a widespread tendency to view political opponents as enemies to be destroyed leading to a willingness to believe the worst about your opponents. Social

media platforms have shown a reluctance to police themselves too aggressively. After it was discovered that a slowed down video of Speaker Nancy Pelosi made her look bumbling, possibly drunk, and out of touch, Facebook refused to take down the video, merely labeling it as fake and something viewers should judge for themselves.[iii] All of these features create a ready-made environment for the online distribution of toxic information.

I. Dirty Tricks Are Not New

The distribution of toxic and misleading information is not new. Before the days of Facebook and Twitter they used to be called dirty tricks. While the medium may be different, the goals are as old as elections themselves. Thus, it is fitting to begin working on the problem of defending democracy in the internet age by trying to understand the world of dirty tricks in the pre-internet age.

To do that, we should distinguish between dirty tricks and negative campaigning, including attack ads and contrast ads. The latter may be offensive but they are based on something that is true as opposed to something that is a wholesale fabrication.

For instance, let's take one of the most infamous ads from the 1988 presidential campaign pitting Vice President George H.W. Bush (R) against Governor Michael Dukakis (D): the Willie Horton ad. It has gone down in history as one of the more offensive and racially incendiary ads ever. Willie Horton, a black prisoner convicted of murder, was released on a prison furlough program in Massachusetts. While out on furlough he kidnapped a young couple, stabbed the man and raped the woman. The ad features a scary photo of Willie Horton and under a photo of Michael Dukakis it says "Allowed Murderers to have Weekend Passes." The weekend furlough program was created in 1972 under a Republican Governor as the result of a court decision. Dukakis himself defended it.[iv]

But both the program and Willie Horton were real. The circumstances surrounding the crime were accurately described, the visual image was true to life even if sensationalized, and there were numerous news stories attesting to the facts of the case.

Now compare this ad to an incident in the 2016 campaign where *nothing* was real: Pizzagate. In the 2016 presidential campaign, social media outlets spread the story referring to campaign manager John Podesta's hacked email accounts that his emails contained coded messages referring to human trafficking and a child sex ring run by high-ranking members of the Democratic Party, including Hillary Clinton. This activity was allegedly based in a Washington, D.C. pizzeria called Comet Ping Pong. The conspiracy theory spread quickly, promoted by various right-wing websites and by the Russians. As the rumors grew so did harassment of the owners and employees of the pizzeria, culminating in a shooting incident by a North Carolina man who took it upon himself to come to Washington and rescue the poor children.

Nothing about Pizzagate was real. There was no sex ring, no coded messages, and no children being held against their will at the pizza place. All the supposed "facts" spread in this story were completely fabricated. The incident illustrates that the difference between dirty tricks and negative campaigning is that dirty tricks are complete lies.

To understand the world of dirty tricks it helps to understand their function in the context of an election. Elections are fought over a finite period of time—Election Day is the endpoint—and public interest increases as Election Day approaches. Unlike a dirty trick against a corporation, which might be remedied in time for a product to rebound, a dirty trick timed to occur before the election can have a definitive impact even if it is proven to be false. The ramifications can be enormous because U.S. elections cannot be re-run.

A brief summary of some of the dirty tricks in American elections shows that they tend to have the following objectives:

- create doubt around a candidate's character;
- confuse the voters about the election;
- break into the opponent's sphere and get information on them;
- affect the actual outcome by interfering with the counting process.

Candidate Character

Sex has long been a favorite topic of the dirty trick. In the early 1800's politics was no less suffused with innuendo than today. Among the most salacious stories were those penned by the partisan journalist James Callender, who alleged in a series of articles that Thomas Jefferson had fathered several children with his young slave, Sally Hemings. For nearly two centuries this was held up as an early example of dirty campaigning. In 1998, thanks to DNA testing, it turned out that Thomas Jefferson had indeed fathered illegitimate children with his slave.

Two centuries later, the combination of illicit sex and race was still the ideal fodder for the creation of a dirty trick. In the 2000 Republican presidential primary then-Governor George Bush of Texas was running against Senator John McCain of Arizona. McCain won the New Hampshire primary and the race went on to South Carolina where the Bush campaign knew they had to stop McCain. Using a tried and true strategy, the phony poll, opponents of McCain spread a complete falsehood. Phone calls to South Carolina Republican voters asked "Would you be more or less likely to vote for John McCain... if you knew he had fathered an illegitimate black child?" McCain and his wife Cindy had adopted a dark-skinned girl from Bangladesh in 1991 and that child, Bridget, was campaigning with them in South Carolina.

Confronted with attacks on their wives and children, candidates have a hard time defending themselves. McCain was distraught at this attack and his efforts to fight back only made his situation worse. He lost the South Carolina primary and the nomination.

His emotional reaction to an attack on his family was not unusual. In 1972, Senator Edmund Muskie was the frontrunner for the Democratic nomination to run against President Richard Nixon. While campaigning in New Hampshire the editor of the all-important *Manchester Union Leader* received a letter from a New Hampshire citizen accusing Muskie of using the word "Canuck," a derogatory term for French Canadians—a significant part of the New Hampshire electorate. Muskie never did any such thing. (The letter was later discovered to have been written by a White House aide to President Nixon, Kenneth Clawson). At the same time, the editor of the *Manchester Union Leader* insulted Muskie's wife, calling her unladylike for drinking too much and telling jokes. Muskie gave a press conference where he was furious and appeared to cry. Whether there were tears or a melted snowflake on his face, the damage was done. Muskie won New Hampshire but by a much smaller

percentage than was anticipated (especially given that he was from a neighboring state.) The narrow victory devastated his candidacy and he lost the Democratic nomination to George McGovern, who turned out to be the weak nominee Nixon preferred.

For much of American history, being gay was a non-starter for a politician. As early as 1836 the hero Davy Crocket wrote that presidential candidate Martin Van Buren was "laced up in corsets, such as women in town wear, and, if possible, tighter than the rest of them." The famous FBI Director J. Edgar Hoover spread rumors that the 1950s Democratic presidential candidate Adlai Stevenson was gay; ironically, Hoover himself has been the subject of rumors and speculation about his sexuality. New York City was the first city which stood up to this tactic. In the 1977 mayoral primary placards appeared out of nowhere that read "vote for Cuomo, not the homo," in reference to Mario Cuomo. Cuomo's opponent Ed Koch won the primary and never directly addressed the rumors about his sexual orientation. These days this line of attack seems almost quaint given the large number of openly gay elected officials, but being a closeted gay may be a sure way to catch the ire of both the gay and straight community.

One of the many problems with complete lies attacking the candidate's character is that they are sometimes so outrageous that the campaign refuses to take them seriously. Or, the campaign knows they are a threat but doesn't want to increase the reach of the dirty trick by giving the lie even more publicity. However, even if a lie is too outrageous for most people to believe, in a tight race only a very small fraction of the electorate needs to believe it. And big lies remind people of the old saying "where there's smoke there's fire." A story that is not plausible on its face may still prompt some to believe that something is wrong with the candidate.

Nearly all of these problems surfaced with the "swift boat" campaign against Senator John Kerry. Kerry had served in Vietnam and was awarded a purple heart, a bronze star and a silver star. In 2004, his service and his heroism in war stood in contrast to President Bush, who had not gone to Vietnam and who got into the Air National Guard through his political connections. Sowing doubt about Kerry's war record was important to the Bush campaign. In the spring of 2004 a group called Swift Boat Veterans for Truth, composed of Vietnam veterans who claimed to have been with Kerry during the incidents

he was awarded medals for, began to hold press conferences and buy television ads questioning each of his medals. A long-time critic of John Kerry (for his later public opposition to the Vietnam War) wrote a book about Kerry called "Unfit for command."

The Kerry campaign's reaction was slow and ineffectual. His top consultants kept restraining him from hitting back out of fear that he would look angry and that it would add even more fuel to the fire. And yet they sorely misjudged the impact the ongoing story was having on cable news during the critical month of August 2004. I was asked to be on Bill O'Reilly show on Fox News during this time. I was not in the Kerry Campaign but as a Democrat was expected to defend him. I asked the campaign for its take on the issue and found there was no response. Susan Estrich, another Democrat, was asked to be on Hannity and Colmes to talk about the ads and had the same experience—there was no help from the campaign.[vvi]

A review of Kerry's war record was conducted by the Navy in September of 2004 and found that the medals were all properly awarded. And Bush himself eventually disavowed the group, but the damage had been done. The big lie only has to sow doubt and the closer the race the more impact it can have.

Confusing the voters

Attempting to confuse the voters is another tried and true characteristic of the dirty trick. Sometimes this is inadvertent but nonetheless critical; the best example being the confusing "butterfly" ballot design that caused voters in the 2000 presidential election in Florida to vote for Al Gore and Republican Pat Buchanan or Al Gore and Socialist David McReynold—thus invalidating their ballots.[vii]

But at other times it is intentional. An early example of intentionally confusing the voters comes from John F. Kennedy's first run for Congress in 1946 in Boston. In Boston then (and now), the two dominant ethnic groups were Irish and Italian and the state was heavily Democratic—meaning that winning the Democratic primary was tantamount to winning the general election. Kennedy, Irish, was running in the Democratic primary against a Boston City Councilor

named Joe Russo, an Italian. Kennedy's father, Joe, allegedly paid another Joseph Russo (this one a custodian with no political experience) to also run in the primary in hopes of splitting the non-Kennedy vote.[viii]

Another way to confuse the voters is to populate the ballot with third-party candidates who are recruited for the express purpose of siphoning votes from the major party. In 2010 a Republican dirty trickster in Arizona got friendly with a group of homeless people and recruited them to run on the Green Party ticket for a variety of offices. Among them were a tarot card reader with less than a dollar to his name who was signed up to run for State Treasurer, a homeless man who went by "Grandpa" on the streets who was recruited to run for the State Senate, and a young street musician who was recruited to run for a seat on the Arizona Corporation Commission. Democrats and Green party officials were furious and filed a lawsuit but failed to get the fake candidates' names off the ballot.

Another tried-and-true dirty trick is to attempt to confuse the voters about important election dates. In the 2018 election Congressman Lee Zeldin (R-NY) sent out flyers telling his constituents that they had to return their absentee ballots by November 6. The actual deadline was November 5 and ballots received after that were not counted. Democrats were suspicious that the "mistake" was meant to keep students from voting but Zeldin's campaign denied any wrongdoing and provided a statement from the printer also saying it was a mistake. The problem was that the Zeldin campaign made the same "mistake" in 2016 as well, fueling suspicion that this was a dirty trick.
In 2012 Wisconsin Democrats, furious over Republican Governor Scott Walker's attacks on public-sector unions, mounted a successful recall petition creating a new election. The 2012 recall election was contested between Walker and Democrat Tom Barrett. As the June 5, 2012 primary date approached, voters reported receiving robocalls (a favorite tool of dirty tricksters) that told voters that if they had signed recall petitions they were not required to vote in the recall election. Walker won the race with 53 percent of the vote.

Breaking and Entering

As we now know, breaking and entering can be physical or digital. The most famous physical breaking and entering was the break-in at Democratic National Committee Headquarters on June 17, 1972, at the Watergate Building in Washington D.C. This began a two-year-long investigation that revealed how President Richard Nixon's CREEP (the appropriate acronym for the Committee to Re-elect the President) used a wide range of dirty tricks to assure Nixon's re-election in 1972. Because the burglary was bungled and immediately publicized in the Washington Post, we'll never know what sorts of information the burglars were after or how they intended to use it in the fall campaign. But the unraveling of that break-in revealed other break-ins—including the break-in at Daniel Ellsberg's psychiatrist's office—and a plethora of dirty tricks carried out by the "plumbers," a group dedicated to finding dirt on Nixon's opponents.[ix][7]

In 2016 a group of Russians, known as the Internet Research Agency, broke into the Democratic National Committee's email system and into the Clinton campaign's email system. They released this information to Wikileaks, who released it to the world in time for the start of the Democratic Convention. The information was damaging enough to cause the resignation of the DNC Chair, Congresswoman Debbie Wasserman-Schultz, and to spread discontent among supporters of Senator Bernie Sanders just when the party should have been uniting for the general election.

Interfering with the election count

Fraudulent election activity is certainly not new to American politics. In the era of big-city political machines it was not unusual to "vote the dead"—have someone go to the polls and vote using the identity of someone who had died. And over the years, candidates and parties have engaged in all sorts of voter fraud—from paying people to vote who had already voted or who were pretending to be someone else to reporting precinct totals with intentional "errors."

In his first run for the United States Senate, Lyndon Johnson, who was later to become president, lost the Democratic primary (that was all you had to win to win Texas in those days) amidst reports of widespread voter fraud. And so, as the story goes, when Johnson got the chance to run again in 1948 against former Governor Coke Stevenson, he was determined to play the game as it

was currently played in Texas. The race became humorously known as the "87 vote landslide." That was Johnson's margin, totally the result of a late-reporting precinct from the town of Alice, Texas. Apparently 202 Mexican-American voters, some deceased or absent from the county on election day lined up at the last minute to cast their votes for Johnson. The ballot box from precinct 13 has mysteriously disappeared and is still sought after.[8]

II. Fast Forward to the Internet Age

Every dirty trick that was possible before the internet is possible today. The biggest difference is that they are cheaper, faster and easier to hide. Plus, the digital age opens up opportunities for new attacks. For instance, with digital technology, it is easy to blend images of particular candidates espousing liberal positions with pictures of leaders in Cuba or Venezuela, and claim their views are outside the American mainstream. Likewise, President Trump's penchant to praise authoritarian leaders in other countries such as North Korea, the Philippines, and Russia opens him to digital strategies tying him to outlandish acts, real or imagined.

It is possible to win elections not just through political persuasion but by convincing important blocs of voters that their preferred candidate is a dishonest career politician out for him or herself and it therefore is a waste of time for them to vote. If you can get enough people in swing states not to vote or waste their ballot on a third-party candidate, it is possible to triumph politically. In this type of situation, one can imagine digital suppression activities targeted on key voting blocs. Opponents can play to common stereotypes and convey appeals based on people's hopes or fears. They can develop false information that leads individuals to be cynical and not to vote. In a close election, those strategies could tilt the contest one direction or another.

There are a wide variety of ways that the vote count itself could be compromised. Many people wonder why we can't vote online and the answer is simple. Small errors, intentional or otherwise, in the software code could, for example, delete every seventh Democratic or Republican vote. Or entire precincts could disappear in the transmission of results from precinct to county or county to state. In fact, the possibility of digital mischief in counting the vote is so noteworthy that many states have disconnected voting machines from the internet and are going back to paper backup ballots to be used in the case of a recount.

Tampering with voter registration data is another option for mischief in the digital age. According to the FBI, Russians successfully infiltrated registration data in at least two Florida counties during the 2016 election. Since that is the information source which election officials use to determine who is eligible to vote, it is an ominous vulnerability. Foreign agents who gain access to registration databases could alter information, disqualify voters, or otherwise create electoral havoc.

Finally, weaponized digital tools can weaken the ultimate winner by casting doubt on his or her legitimacy. The United States has convoluted election rules and it is possible to create doubts through a number of different scenarios that analysts say are possible in 2020. For example, commentator Jeff Greenfield describes three ominous options: a state legislature rejects the popular vote and casts its Electoral College votes the way it wants (as opposed to in line with the votes in the election), the U.S. House of Representatives refuses to accept votes from particular states, or the absence of an Electoral College majority tosses the race into the House, where each state delegation has one vote. With Republicans holding a majority of state delegations, there is a good chance under this scenario the House would choose the GOP candidate as the next president.[x]

With any of these results, it is easy to see a number of Americans not accepting the ultimate electoral result as legitimate and seeing the verdict as unfair or unjust. They could conclude the winning party used nefarious means to produce a victory. They could see the results as completely tainted and therefore not accept the authority of the resulting administration.

III. Who Can Protect America's elections and How?

When it comes to fighting illegal intrusions into American elections, the states and localities are where the rubber meets the road—that is where American elections are administered. This authority is grounded in more than tradition; it derives from Article I, Section 4 of the Constitution. That section notes that while Congress has the authority to intervene in the setting of elections, election administration is largely a function of state and local government.

Given this situation, election law and practice vary considerably from state to state, which leads to a number of ramifications. On the one hand, this decentralization makes it hard for a single cyberattack to take down the entire American election system. But having a fragmented system poses some disadvantages as well. Some states and localities are simply better equipped to protect against cyber intrusions than others, and an adversary seeking to sow doubt and confusion about the integrity of an election needs to compromise only a few parts of the entire system in order to undermine public confidence.

The vulnerabilities in election administration exist at every step of the process, from the registration of voters, to the recruitment of poll workers for election day, to the books of registered voters at polling places, to the devices that capture and tally the vote, to the transmission of that data to a central place on election night and to the ability to execute an accurate recount. Every state and locality want to run a fair election but they are limited by inadequate funding, the absence of trained personnel, and outdated technology.

A 2019 bipartisan report out of the Senate Intelligence Committee concluded that,

> "In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain."

The Committee also found that the Russians had attempted to intrude in all 50 states, an assessment that went far beyond the original claim. And 2016 was not the end of it. A few weeks before the 2018 midterm elections the Department of Homeland Security (DHS) found that numerous actors were routinely targeting election infrastructure. Warnings continue that in the next election attacks could be coming not only from Russia but from other actors as well. Most recently, the former Special Counsel Robert Mueller made headlines when he told Congress "They're [the Russians] doing it as we sit here."

So, what are states doing in preparation? They are hardening their election infrastructure, training election personnel, testing their systems and providing backup. But it is not clear these steps will be sufficient. For example, state systems for registering voters are ripe targets for those who would seek to sway an election or simply sow chaos. The inviolability of the voter registration system is critical to making sure that everyone who wants to vote is able to vote. In July of 2016 twelve Russians hacked into the election database of the State of Illinois. They stole data on about 76,000 voters. Once it was noticed, the assault caused the state to close down their online voter registration website, which turned out to be the result of a hole in the system.

Once voters register, their information is distributed to polling places around the state. If voters' names have been erased or changed they will be unable to vote or forced to file a provisional ballot—creating delay and confusion in the vote count. Harvard University's State and Local Election Cybersecurity Playbook recommends (among other things) that systems are patched and updated and that the database is not accessible over the public internet. Electronic vulnerabilities exist with voting machines as well as with voter registration systems. In July, 2017 hackers at the DefCon hacking conference invaded 30 Direct Record Electronic (DRE) touch-screen voting machines. (Defcon is one of the largest hacking conferences in the world.) The state of Virginia, facing an important gubernatorial election, decertified the vulnerable machines leaving more than twenty cities and counties scrambling to get new equipment in time for their gubernatorial election.

In addition to upgrading their infrastructure and increasing the security around it, states are looking for ways to better train election personnel. For some time now, concern has centered on the front-line personnel in the election system: poll watchers. With 116,990 polling places and 8,616 early voting locations around the country, states have a hard time recruiting poll workers. In addition, many of them are elderly. In 2017 the U.S. Election Commission found that 56% were age 61 and older and that states were trying to recruit some younger poll workers who are more comfortable with technology.

Finally, the many threats to elections have increased attention to ways of validating election results. The first is (ironically in this day of paperless everything), the re-introduction of paper ballots in the election system and the second is the mandatory risk-limiting audit. Because electronic tabulation

systems are vulnerable to all sorts of electronic mischief, the need for post-election verification is more important than ever. Paper ballots are the only way a state has of conducting either a recount or an accurate audit of an election. Following the decertification of some of its election machines, the State of Virginia adopted a system where paper ballots would be marked, fed into a scanner and then saved, if needed, for a recount. Many more states have gone back to paper. Fourteen states now require paper ballots, and another seventeen require voting machines to have a paper record verified by the voter himself or herself. Six states require their machines to have a permanent voter record. Thirteen states do not have a statutory requirement, nine of them have a statewide paper trail and the remaining have some jurisdictions with a paper trail and some without.

There is a certain historic irony to this return to paper ballots. Many Americans can remember the confusion created by the paper ballots that were used in the contested 2000 election in Florida. As a result of that election, the Help America Vote Act helped states replace their old machines with DRE (Direct Recording Electronic) systems. These systems, even if not connected to the Internet, are easily compromised, as proven by the hackers at Defcon.[xi]

Paper ballots allow a state to conduct what's known as a "post-election audit." In those states that use a traditional type of post-election audit, officials hand-count a certain portion of the ballots and compare the results to the ones produced by the electronic voting machines. A more recent type of audit is called the "risk-limiting audit," in which statistical methods are used to cut down on the number of ballots that need to be checked. If the electronic margin is large, fewer ballots need to be examined. If it is small, more ballots need to be looked at. The audit "either (a) stops when it finds strong evidence that the reported outcome is correct, or (b) fails to find strong evidence that the outcome is correct and evolved into a full hand count of ballots." According to a study from MIT, the risk-limiting audit "does not stop auditing until and unless there is strong statistical evidence that a full hand count would simply confirm the reported outcome."

States and localities are on the front lines of protecting our elections. They are taking, along with the federal government, important steps to secure and upgrade their election infrastructure. But this cannot be a one-time activity. In the digital age, once one door is closed to the hackers, they go in search of

another—the need to protect election systems will be ongoing. In a close election, a miscreant could compromise the entire result by hacking or disrupting a few counties in a couple of crucial states. It doesn't take much to cast doubt on the entire process – which is why the Federal government is also critical.

The Federal-State disconnect

Although the U.S. federal government is not the leading actor in the administration of elections - the federal government is the leading actor in protecting the country from foreign attack. Thus, when America's election infrastructure is attacked by a foreign entity, responsibility for election cybersecurity falls to (or in between) both federal and state governments. In the federal government the two biggest players are the Department of Defense (DOD) and the Department of Homeland Security (DHS), and within them the U.S. Cybercommand (created in 2010) and the Cybersecurity and Infrastructure Security Agency (CSIA), respectively. But there are other actors as well. The intelligence services, especially the ODNI (Office of the Director of National Intelligence) NSA (National Security Agency) and, of course, the CIA (Central Intelligence Agency) have a large role to play in identifying threats abroad. (The detailed indictments of Russian individuals involved in hacking operations in the 2016 elections would not have been possible without a certain amount of old-fashioned spying.) The FBI also has a role to play in tracking down those who commit crimes here. And NIST (the National Institute of Standards and Technology) has a role in cybersecurity through its mission of promoting U.S. competitiveness and innovation.

As we discovered post 9/11, the federal government has huge capabilities which are spread over many different parts of the government. In the aftermath of the 9/11 attacks, high-level commissions were formed and studies were conducted to figure out what went wrong. It became clear that one of the biggest problems with these huge capabilities was the inability of people in different agencies to share information in a timely and effective fashion. Pieces of information that, had they been put together, may have prevented 9/11 were spread over a wide variety of agencies who didn't talk to each other. Thus "connecting the dots" became the catchphrase of the post-9/11 efforts at reform as the federal government's domestic and international capabilities were encouraged to share information to better cooperate in the war on terror.

An analogous problem occurred in 2016. This time the federal government, especially DHS and FBI, had to interact with state governments in order to advise them that their election systems were under attack. According to the Report of the Select Committee on Intelligence, the communication and cooperation went badly. The interface between the federal government and the state governments was not seamless; confronted with a new and poorly understood threat, there were missed signals on all sides. To begin with, CSIA was founded to provide cyber protection to all forms of infrastructure, from power plants to elections. But, as one state official told the Senate Committee "DHS didn't recognize that securing an election process is not the same as securing a power grid."

That gap led to a variety of problems with federal government attempts to help the states. For instance, the federal government alerted the states to attempted intrusions in the summer of 2016 but failed to tell them that the intrusions were attempts by a hostile foreign power. Since election infrastructure, like the infrastructure in other sectors, is under constant attack, many of the officials alerted didn't regard the notice as particularly important and in some instances state IT directors failed to alert elections officials about anything unusual. Both sides had problems understanding each other. Since responsibility for elections is dispersed among and within states, federal officials often spoke to the wrong people. And on the other side, since very few election officials had security clearances, federal officials didn't feel they could "read in" officials to the true nature and thus severity of the attempts on the state election's infrastructure. The Senate Intelligence Committee concluded:

> "The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials."

Much of the disconnect that occurred in 2016 was the inevitable consequence of the unprecedented attack by Russia on America's elections. In the intervening years, all the players, from the federal level to the local level have gotten more sophisticated and more attuned to the new threat. Just as 9/11

opened America's eyes to the threat of terrorists using airplanes as bombs, 2016 opened America's eyes to the threat aimed at the very heart of our democracy. Three years later all the agencies with a piece of cyber security were alerted to the threat; training, war gaming and the use of "red teaming" were all part of the federal government's operations.[1]

But one essential element to getting the federal government's vast resources to the states was the issue of security clearances. In order for state election officials to hear and understand the full potential impact of the threats they are under, they need to have security clearances. According to the Senate Intelligence committee: "... the story of Russian attempts to hack state infrastructure was one of confusion and a lack of information. ...At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor." The lack of information flow in 2016 is largely due to the fact that at that time almost no state election officials had security clearances and were thus not privy to understanding the full extent of the threat posed by the Russians.

The timely issuance of security clearances is a long-standing and thorny problem for the federal government. It has gotten so bad that in January 2018, the Government Accounting Office (GAO) placed the National Background Investigations Bureau on its infamous "High Risk List," a list devoted to pointing out the government organizations with the biggest operational problems. "The backlog of people awaiting clearances ballooned from 190,700 in August 2014, to 581,200 in April 2017 and more than 700,000 in September that year. The Office of Personnel Management's goal for a stable backlog is 180,000 cases."

Without a rapid increase in the issuance of clearances, the missed signals and incomplete information that characterized the federal-state relationship in 2016 is apt to happen again. Important, malicious intrusions are likely to be missed, while intrusions from a 14-year-old with a laptop are likely to be paid inordinate attention.

The old saying goes "Fool me once, shame on you; fool me twice, shame on me." The 2020 federal government is likely to be better prepared and more sophisticated than they were in 2016. But they will still need the ability to communicate threats in a comprehensive manner and getting state and local officials the proper clearances is central to that task. Which brings us to the problem of leadership.

IV. Leadership

State and Federal governments are stepping up to the problem of cybersecurity in American elections but they are doing so within their existing authorities and without executive or congressional leadership.

From the very beginning of his presidency, Donald Trump has denied or downplayed Russian interference in the 2016 campaign. He has, at various times, dismissed the whole idea as a hoax, as fake news, or as an excuse by Democrats for why they lost the election. At other times, he has proclaimed his innocence vis-à-vis Russian campaign interference. From the earliest days of his presidency when he fired FBI Director James Comey in an effort to stop the investigation, he has denigrated and dismissed the entire issue. In its place he has insisted that the real problem in 2016 was not Russian interference but rather illegal voting by immigrants. The president's beliefs have put him at odds with his own government and his own appointees, creating some awkward moments as the machinery of the federal government comes into conflict with the tweets of the chief executive.

In spite of the president's antipathy towards the effort, the gears of government managed to grind on, even in the White House. On September 12, 2018, President Trump issued Executive Order 13848 titled "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election." The order requires a post-election audit by the intelligence community, under the direction of the ODNI (Office of the Director of National Intelligence) and mechanisms to place sanctions—such as confiscation of property—on those who take actions to interfere in U.S. elections.

Executive Order 13848 was dismissed by many Democrats and some Republicans as inadequate. But it highlighted the sensitivity within the federal government to the president's stance. First note the wording "in the event of foreign interference," which indicates that interference may not happen after all—a contradiction of the opinions expressed by many in the intelligence community. Second, in 2016, disinformation campaigns by the Russians were more successful than their attempts to break into election infrastructure, but the order is narrowly drawn to focus on election machinery and leave out disinformation efforts.

The president's hostile stance became public in April of 2019 when the Secretary of DHS Kirstjen Nielsen was told not to bring up election security in front of the president. Nielsen had been pushing for a White House-led Cabinet meeting on securing the 2020 elections. While DHS has the lead, election security crosses many federal government departments. A Cabinet-level meeting would help put the issue front and center. But the Secretary's attempts were foiled and she was forced out that same month.

Other parts of the federal government besides DHS are critical to election security as well—particularly the intelligence community. In January 2019, the Director of the Office of National Intelligence, Dan Coats, delivered an annual Threat Assessment. This exercise is designed to prioritize the threats facing the nation that have been gleaned from the various intelligence agencies. The first threat he mentioned was election security: "We assess that foreign actors will view the 2020 U.S. elections as an opportunity to advance their interests." Election security topped threats from China, Russia, North Korea and Iran, which, the DNI noted, are all advancing their cyber-capabilities. Predictably, the report made the president angry—although his anger appeared directed as much at their assessment of the Iranian threat as their assessment of other threats. Once again, the president attacked the intelligence community, telling them in one tweet to go back to school.

Trump's allies in the Congress have also been hostile to the election security issue. Immediately after former Special Prosecutor Robert Mueller delivered his clear-cut warning to the nation that the Russians were already actively attempting to interfere in elections, Senate Majority Leader Mitch McConnell blocked two bills, calling them "partisan."

McConnell's actions caused the Washington Post columnist Dana Milbank to call him a "Russian asset." Then MSNBC's Joe Scarborough dubbed him "Moscow Mitch," a name that Speaker Nancy Pelosi (D-Calif.) picked up and used in a speech. The moniker quickly went viral, irritating the majority leader and highlighting the Republican leader's legislative inaction.

Trump and McConnell's hostility to cyber protection is unfortunate given that there are many good ideas to protect and improve American election administration. Four major pieces of election security legislation have been introduced over the last two years: the Secure Elections Act (introduced by Senators James Lankford (R-OK) and Amy Klobuchar (D-MN)); Defending American Security from Kremlin Aggression Act (introduced by Senators

Lindsey Graham (R-SC), Bob Menendez (D-NJ), Cory Gardner (R-CO), Ben Cardin (D-MD), and Jeanne Shaheen (D-NH)); Defending Elections from Threats by Establishing Redlines Act (Senators Marco Rubio (R-FL) and Chris Van Hollen (D-MD)); and Securing America's Federal Elections Act(introduced by Representative Zoe Lofgren (D-CA19)).

As noted below, the bills demonstrate relative bipartisan agreement over several key remedies. A number of members have proposed providing additional funding for the Election Assistance Commission, sharing election security expertise with the states, providing paper ballot backups of electronic voting systems, sanctioning financial institutions that support foreign interference, authorizing retaliatory actions against any nation interfering in American elections, and requiring intelligence agencies to determine whether any foreign agents interfered in American elections. A version of these ideas already has been approved by the U.S. House of Representatives on a 225 to 184 vote, but has been repeatedly blocked from a Senate vote by Senate Majority Leader McConnell (R-KY). Calling the bill "highly partisan," McConnell blocked a unanimous consent vote on the bill just hours after Mueller's testimony

In looking across the proposed bills, there are a number of promising ideas designed to secure U.S. elections.

Providing additional funding for the Election Assistance Commission

One of them advanced in the Secure Elections Act is the creation of an Election Assistance Commission grant program that provides funding for states and localities to secure electoral processes and upgrade equipment. The idea is that since elections largely are administered at the state and local level, additional funding for those entities would enable them to update their equipment, install the latest cybersecurity protections, and make sure that vital infrastructure is protected during the election.

Sharing Election Security Expertise

Several of the proposed bills give the U.S. Department of Homeland Security (DHS) a bigger role in advising the states, offering them technical expertise, and being proactive in dealing with possible cyber-threats. Since this department works to counter terrorism and maintain vital infrastructure, the department has expertise to evaluate hardware and software for cybersecurity

risks. Armed with that information, it could provide help to state and local agencies charged with administering the upcoming elections.

Providing paper ballot backups of electronic voting systems with an audit trail

A number of local jurisdictions have moved to electronic voting machines in recent years, although in most cases, this equipment is not connected to the internet in order to minimize opportunities for hacking. However, there still could be software bugs that distort the vote or systematically undercount certain areas. Given that possibility, it is important to have paper ballot backups of electronic voting systems and the possibility of conducting an audit if any irregularities are spotted. That way, voters can feel confident their votes will be counted and there are mechanisms to evaluate the vote in case anything is contested.

Sanctioning financial institutions that support foreign interference

The Defending American Security from Kremlin Aggression Act establishes financial sanctions that could be applied against countries, financial institutions, or individuals that "facilitate illicit and corrupt activities, directly or indirectly, on behalf of Putin." The idea is that Russians could be discouraged from malicious behavior if they think there will be serious consequences.

In addition, the bill "would give prosecutors additional authorities to pursue federal charges for the hacking of voting systems and create a National Fusion Center to respond to hybrid threats of disinformation and other emerging threats from Russia". There are provisions that specifically would impose sanctions for "Russian interference in democratic processes."

Authorize retaliatory actions against any nation interfering in American elections

The Defending Elections from Threats by Establishing Redlines (DETER) Act would allow the President to impose sanctions against any country identified as a threat. Among the actions that could invite retaliation "include a foreign government or agent purchasing political advertisements to influence an election" or "using social media to spread false information, hacking and releasing or modifying election- or campaign-related information or hindering access to elections infrastructure, such as websites for polling places."

Requiring intelligence agency leaders to determine whether any foreign agents interfered in American elections

The DETER Act would mandate that the director of national intelligence determine within 30 days of the national election whether "the government of a foreign country, or any person acting as an agent of or on behalf of that government, knowingly engaged in interference in the election." Under threat of sanction, foreign agents specifically would not be allowed to "spread significant amounts of false information to Americans. They also cannot hack, leak or modify election and campaign infrastructure, including voter registration databases and campaign emails."

Instead of passing legislation that would enhance the federal role in protecting elections, Trump and McConnell have stood firm against any large scale action on this front. A number of arguments have been made to justify the votes of those who opposed the House bill or are supporting Senate inaction. One is a state's rights argument suggesting that the federal government should not have a major role in electoral security given the country's history of state and local control of balloting. While it certainly is important to maintain state and local control of elections, providing federal assistance to upgrade voting machines does not violate existing legal or constitution provisions. There is a long history of the federal government paying for voting equipment and offering technical assistance. Many states lack funding for voting machines and the federal government often has funded upgrades and improvements. There is ample precedent for national authorities to protect vital infrastructure in the face of foreign threats.

Another rationale concerns the financial cost of electoral security. The idea is at a time when America is running a trillion-dollar budget deficit, it should avoid unnecessary expenditures. Rather, lawmakers should focus on vital priorities and critical infrastructure. Yet electoral security should fall within each of those principles. Having secure elections is essential to democracy. There is no excuse for not spending several hundred million dollars (a very small portion of the overall federal budget) on meaningful steps to protect American elections. Democracy is too important to be risked for a relatively small amount of money. Congress did appropriate $380 million in election security grants to states before the 2018 elections. Little of that was spent however, because the money came so late—but many states are planning to spend the

rest in preparation for 2020. The FY 2020 appropriations bill passed out of the House provides for another $600 million in election security grants to "augment state efforts to improve the security and integrity of elections for Federal office." But this bill needs to be passed in a timely manner in order to have a real effect.

The absence of leadership on this issue is extremely dangerous. But no matter how many governments and law enforcement agencies are scrutinizing elections for illegal interference, candidates, campaign staffs, and party officials are likely to be the first to notice malicious interference.

V. Political Campaigns are the first line of defense in election security

Disinformation campaigns, voter suppression efforts, and interference with the vote count are likely to be caught first by campaigns because they consistently monitor all three.

Most large, sophisticated campaigns routinely set up "war rooms" or "rapid response" units that monitor news and social media around the clock and prepare to answer attacks on the campaign. Round-the-clock monitoring applies to their opponents as well. Thus, campaigns are likely to notice disinformation campaigns that are against them *or that advantage them* before anyone else does. Second, going into a campaign, candidates and parties have a very good idea where their votes should be coming from and by what margins. They therefore are likely to notice attempts at voter suppression (traditional or digital) long before anyone else does. Let's look at each one in turn.

Disinformation

The 2016 presidential election was filled with negative disinformation about Hillary Clinton that originated with the Russians. From "pizzagate" (the ridiculous assertion that Hillary ran a pedophile ring out of a pizza parlor in Washington D.C.) to her having Parkinson's disease to the candidate making a small fortune by arming ISIS, the negative stories were fast and furious. Many were targeted to supporters of Bernie Sanders, both in the primary and in the general election. Sanders' supporters, notably four volunteer web administrators, noticed something funny on their sites and alerted their followers that they were being fed disinformation. One of them, Matthew Smollon, a web administrator from Knoxville, Tennessee, posted the following to his supporters in June, 2016,

> "Guys, I sincerely love you. I love your passion. I love your fire. I love all of that. But when 400 people are circle-jerking clickbait links in between wondering how Hillary Clinton is behind the FEMA Earthquake drill that happens on several days with one of them being primary day? Holy shit. You are allowing yourselves to be manipulated. Through the practice of taking anything that agrees with your opinion at face value, actively refusing to believe anything but what agrees with your narrative and following that up with blatant disregard for doing two minutes of searching to verify the information: you become the myopic Trump supporter that you so vocally loathe."

Nearly two years after Sanders' web administrators noticed suspicious, anti-Hillary activity on their sites, the Mueller indictments confirmed that the Russians were out to help Donald Trump *and* Bernie Sanders. This put Sanders himself on the defensive and in February of 2018 he went on the NBC-TV interview show "Meet the Press," claiming one of his staffers had alerted the Clinton campaign to the fact that "something weird is going on." The statement was not quite accurate. In fact, one of his volunteer web administrators, John Mattes of San Diego, had communicated with a PAC supporting Clinton but not with the actual campaign.

The fact that at least some parts of the Sanders' campaign knew about Russian interference brought up a bigger issue and one that is likely to be with the political world for some time: what is the responsibility of a campaign when it is being advantaged by disinformation?

In August 2018, at the summer meeting of the Democratic National Committee, I in conjunction with former Party Chairwoman Donna Brazile and the North Carolina delegation to the DNC submitted a resolution which was passed by the full DNC. In addition to asking campaigns to be vigilant about monitoring, identifying and disclosing malicious activity it urged candidates to "inform the public of attacks on our electoral process as soon as possible and when such disclosures would not interfere with ongoing investigations." In advance of the midterm elections, the Democratic National Committee Chair, Tom Perez, engaged the Chair of the Republican National Committee, Ronna McDaniel, in an effort to get both sides to pledge not to use hacked material in

the 2018 cycle. But talks broke down over whether or not a party's candidates could use hacked material that had been in the press.

A year later all the Democratic hopefuls in the presidential race, including Sanders, and the Democratic National Committee itself had declared that they would not take advantage of illegally obtained information. Meanwhile the Trump campaign declined to make any such promise and Rudy Giuliani, Trump's attorney, stated that there was "nothing wrong with taking information from the Russians" and has been information from Ukraine on at least one of the leading Democratic contenders.

Voter suppression

The second place where campaigns are likely to encounter malfeasance is in the area of voter suppression. Voter suppression is as old as American history itself and has focused for centuries on the African-American vote. The 21st century saw a resurgence of efforts to suppress the African-American vote but in addition to more traditional efforts in recent elections we saw digital voter suppression. The Trump campaign set out to suppress the vote of three voting blocs. In an article written before Election Day 2016 Joshua Green and Sasha Issenberg pointed out that unlike most campaigns, the Trump campaign was seeking to shrink rather than expand the electorate. In the piece they quote a senior official in the Trump campaign as follows:

> "We have three major voter suppression operations under way. They're aimed at three groups Clinton needs to win overwhelmingly: idealistic white liberals, young women and African Americans."

Using "dark" ads which only the recipients could see, the Trump campaign urged Bernie Sanders voters to vote for Jill Stein and they reminded black voters that Clinton had once called gang members "super-predators." They also had women who had accused Bill Clinton of sexual misbehavior attend a debate in an effort to counter Trump's own sexual misdeeds and neutralize women who might vote against him.

The Trump voter suppression campaign was, however, only the tip of the iceberg. Again, as detailed in the Mueller indictments, the Russians sought to suppress the vote among Bernie Sanders voters and among African-

Americans, with ads such as "Hillary Clinton Doesn't Deserve the Black Vote" and "You know, a great number of black people support us saying that #HillaryClintonIsNotMyPresident."

Hillary Clinton's election models had been built on certain expectations, well-founded historically, about how the black community would turn out and vote. But two things happened on election night that proved the models wrong. Across the board in the United States, African-American turnout was down. More importantly, in two of the three critical states Clinton lost to Trump, the distance in the African-American vote for Hillary compared to Barack Obama in 2012 *exceeded Trump's margin of victory in the state*. In Wayne County, Michigan, home of Detroit, Obama got 595,846 votes in 2012 and Clinton got 519,444 votes in 2016 for a difference of 76,402 votes—seven times more than enough votes to have swung the state to Clinton had she performed as Obama had four years earlier. And in Milwaukee County, Obama got 332,438 votes in 2012 and Clinton got 288,822 (this is after the recount) for a difference of 43,616 votes—nearly twice what would have been needed to carry Wisconsin for Hillary.

Tabulating the vote

The final way in which candidates and campaigns are on the front lines of election security is in the tabulation of the vote. Campaigns, especially at the presidential level, have very finely tuned expectations of the votes they need to win. Large differences from those totals can be a clue to possible interference in the tabulation of the vote.

On election day 2016 the final vote totals in three critical states differed from the exit polls, from the models and from the candidates' own polling. However, as far as we know, there was no interference in the vote tabulation in 2016. Per the Senate Intelligence Committee report, "The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election day, though again the Committee and IC's [Intelligence Community] insight into this is limited." However, the Committee did find that Russians attempted to hack into the election systems of all 50 states—more than double than what had been assumed just a year before. It appears that the Russians conducted mostly scanning of election-related state infrastructure.

One of the earliest reports of something odd happening came out of Illinois where there were repeated and successful attempts to hack into the Illinois' online voter registration system. They appear to have stolen the identities of about 500,000 voters but it doesn't appear that they actually managed to delete voters' registration or to change votes.

However, the attacks on election infrastructure could be used to gather information about the system and about vulnerabilities that will be used in a future election to penetrate the system and change votes or change vote tallies. In that case the campaign would likely spot unexpected results—unless of course, the penetration was so carefully done that it veered only slightly from the campaign's own expectations of the vote. In that case, skewed tabulations might be impossible to catch.

VI. Looking ahead

While Americans have varying opinions on the threat of foreign interference in the 2020 elections, they do want Congress to take meaningful action. Researchers at Brookings conducted on online poll in August 2019.[xii] When asked how worried they are about interference in 2020, 28 percent say they are very worried, 19 percent are somewhat worried, 35 percent are not very worried, and 18 percent are unsure.

In spite of the varying opinions about the foreign threat, many Americans want Congress to take meaningful action. Fifty-eight percent believe the U.S. government should provide additional funding to the states to help them upgrade the security of their election equipment, 19 percent do not, and 23 percent are unsure. Sixty percent also think the U.S. government should offer additional technical expertise to the states to help them upgrade their electoral machines, 17 percent do not, and 23 percent are unsure. The poll also found that people want the technology firms to do more to fight foreign interference and that Russia is the country of greatest concern.

Yet the risk of foreign intervention goes far beyond Russia. Indeed, this type of action has happened many times in U.S. history. In 1796, for example, rivals England and France contested the presidential campaign on opposite sides of the race. Smarting from its defeat in the American Revolutionary War just a few decades earlier, England saw the Federalist John Adams as more sympathetic to its side, while France favored Thomas Jefferson, who had served as the U.S. Ambassador to the French in President George

Washington's administration and was more open to the aspirations of the French Revolution.

In 1940, Germany encouraged Charles Lindbergh's isolationist sentiments against President Franklin Roosevelt. It saw isolationism as a way to keep America from providing material support and entering the war on the side of France and England. Later, the Nazis unsuccessfully tried to help Republican nominee Wendell Wilkie through releasing documents hostile to Roosevelt.

In 1984, the Soviet Union was not happy with U.S. President Ronald Reagan. Its leaders saw him as bellicose and militaristic, and boosting defense spending at an alarming rate. In an effort to find material that might undermine the president, it spied on the Republican National Committee, but did not find anything that stopped Reagan's reelection.

In 1996, there were allegations of illegal Chinese campaign contributions to the Democratic National Committee. At the time, China was worried about hostile policies from the Republican party and thought President Bill Clinton was more supportive of its economic development plans. It was a crucial time in Chinese history because its government was edging towards more international trade and wanted to be sure Western nations would not block its growth.

What's new in 2020 is that, over the past few years, Russians have shown other nations how easy it is to sow disinformation and disrupt democratic elections. Many countries, including the United States, seek to make the voting process easy so balloting is designed much more for user-friendliness than electoral security. At the same time, technology companies have created social media platforms that are easily exploited through disinformation, false news, and fake videos. What's more, the use of this technology to disrupt campaigns is cheap and difficult to trace.

The stakes of the upcoming election extend way beyond the shores of the United States. Due to its global impact, what happens in America has tremendous implications for other countries. Our policies affect the economic development opportunities, competitiveness, and security of other places. U.S. actions increase incentives for foreign entities to seek to influence the

U.S. campaign. It matters considerably to other nations who wins and what happens in terms of U.S. foreign and trade policies. The economies of other nations will rise or fall depending on who emerges as the next American president.

Recognizing this possibility, President Trump has baited China with an August 1 tweet saying "China, Iran & other foreign countries are looking at the Democrat Candidates and 'drooling' over the small prospect that they could be dealing with them in the not too distant future. They would be able to rip off our beloved USA like never before."

His taunt raises the prospect of foreign campaign intervention in 2020 may extend way beyond Russia to countries such as China, Iran, North Korea, Saudi Arabia, and others that have a major stake in the electoral outcome. Foreign governments recognize there will be differences between dealing with Trump, Joe Biden, Elizabeth Warren, Bernie Sanders, Kamala Harris, Pete Buttigieg, or Cory Booker as the next American leader. Each has different values, policies, and visions that will impact foreign lands.

In an interview on Rachel Maddow's MSNBC television show, Hillary Clinton anticipated a scenario of other governments contesting the American election. She raised the prospect China may try to undermine President Trump by saying "China, if you're listening, why don't you get Trump's tax returns? I am sure our media would richly reward you."

In an interview on Rachel Maddow's MSNBC television show, Hillary Clinton anticipated a scenario of other governments contesting the American election. She raised the prospect China may try to undermine President Trump by saying "China, if you're listening, why don't you get Trump's tax returns? I am sure our media would richly reward you."

Imagine a 2020 campaign where Russia, Saudi Arabia, and North Korea engage in U.S. activities designed to re-elect Trump while China, Iran, and others seek to undermine him. Americans could wake up the day after the election not knowing whether they were manipulated into an election outcome by direct or indirect foreign activities. The mere possibility of that happening should unsettle all Americans.

In the lead-up to the 2020 election, many nations worry whether a second Trump term will advantage or disadvantage them. China is in the midst of a trade war launched by President Trump. Iran sees Trump as openly hostile to its interests. The Saudi kingdom has benefitted from close ties to the Trump family. North Korea Leader Kim Jong Un has forged a friendly relationship with President Trump and therefore may want to see him remain in office.

While this list could go on to include other countries, including those friendly to the United States, it is clear the 2020 stakes are high in many places around the world. With the Russian disinformation playbook on open display for all to see and use, the ease of intervention may lead to a campaign contested by many foreign agents. U.S. authorities, news organizations, and voters will need to remain vigilant about a wide range of foreign threats.

VII. Conclusion: What Can be done?

This is not an easy problem. It does not have a simple legal fix, nor does it have a technological fix. And yet there are things that can be done to make the 2020 elections safer and more legitimate. Here's a preliminary list.

- Pass the legislation that has been introduced in the Senate that seeks to protect American elections by offering assistance to states, authorizing retaliatory actions against nations interfering in elections and requiring intelligence agency leaders to determine whether any foreign agents interfered in American elections.

- Appropriate money in a timely fashion to help states upgrade their elections systems especially old DRE (Direct Record Electronic) voting machines.

- Incentivize states to make verified paper ballots and post-election audits a part of their regular election administration; and to protect their voter registration files.

- Train volunteer election officials to deal with technology and the dangers of cyber intrusions.

- Create a climate within political parties in which it is *not* acceptable to take advantage of a malicious campaign of disinformation. In a

primary contest the party can even evoke sanctions against the offending candidate—such as keeping him or her off a debate stage. In a general election contest there is little recourse but to try and heap public opprobrium on a candidate who promotes obviously fake information.

- Monitor what a campaign's targeted voters are seeing on the internet. Given the ability to micro-target this may be difficult to uncover unless campaigns have real people on the street talking to prospective voters. That's about the only way to pick up dark ads that are bombarding likely voters.

- Create a cyber security carve out in election law. The Federal Election Commission allows candidates to raise money specifically to offset the cost of legal and accounting services necessary to comply with the law. These funds cannot be used for campaign purposes. The purpose of this special category of contribution is recognition of the fact that these are costly but necessary services. The same argument could be made for creation of a special cybersecurity account to pay for software, consultants etc. to protect a campaign against malicious intrusions. All campaigns should have high levels of cybersecurity but if forced to choose between a new piece of software and one more media buy the choice will often go against cybersecurity.

- Equip candidates with the best security they can. The major political parties should take it upon themselves to equip all their candidates with the best cybersecurity they can afford. Recently the National Republican Congressional Committee announced it would fly their tech team out to candidates' districts to "train their staff to spot suspicious emails and websites, ensure all their software is patched against bugs and set them up with a suite of free anti-hacking tools." This is clearly in the interest of the political parties. They should be allowed to raise money for this purpose outside of raising and spending restrictions and to aid the candidates running on their ticket.

- Create regular "after-action reviews." The political parties should be part of a regular "after-action review" or "lessons-learned debrief" with DHS and the intelligence agencies after every major election. The debrief should be separate for each political party and should be conducted with top civil servants only—no political appointees. The

purpose of these sessions should be to honestly evaluate what the enemy tried, succeeded at, and how the government and campaigns responded.

These efforts alone will not guarantee safe and fair elections. There is always the possibility of electoral mischief either of traditional or digital forms. But adopting these measures will at least move us in the right direction toward protecting the integrity of the 2020 campaign.

[i] Taylor Telford, "'The World Is Not Yet Ready for DeepNude': Creator Kills App That Uses AI to Fake Naked Images of Women," *Washington Post*, June 28, 2019.

[ii] Joseph Cox, "GitHub Removed Open Source Versions of DeepNude," *Motherboard*, July 9, 2019.

[iii] cecilia Kang, "Nancy Pelosi Criticizes Facebook for Handling of Altered Videos," *New York Times*, May 29, 2019.

[iv] https://www.nytimes.com/1988/07/05/us/prison-furloughs-in-massachusetts-threaten-dukakis-record-on-crime.html

[v] See Chapter 6 in *Election 2004: How Bush Cheney '04 won and what you can expect in the future,* by Evan Thomas and the Staff of Newsweek. (Public Affairs, 2004) for a description of the Kerry campaign's inept response.

[vi]

[vii] http://www.cnn.com/2001/ALLPOLITICS/03/11/palmbeach.recount/

[viii]

[ix]

[x]

[xi] For a longer discussion of paper ballots and audits see: https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/

[xii] https://www.brookings.edu/blog/fixgov/2019/08/20/americans-want-federal-action-on-election-security-ahead-of-2020-per-new-brookings-survey/