In 2016, Russia’s interference in the U.S. election shook the nation. Since then, the CIA and FBI concluded with “high confidence” that Russia’s goal was to help Donald Trump’s candidacy and harm Hillary Clinton’s. That said, President Trump has at times denied Russia’s involvement, their intent, and their effect on the election. This article provides an overview of what took place in the 2016 and 2018 elections, and what we know thus far about the 2020 elections. Then, it will cover proposed solutions to protect American elections from cyber interference in 2020 and beyond.

Election Interference in the U.S. Since 2016

2016 Presidential Election

Russia’s interference attempts in the 2016 election can be categorized into four discrete efforts: (1) hacking of servers (2) email phishing schemes (3) misinformation through social media and the internet (4) attempted hacking of voting machines.

The first sign of Russia’s interference in the 2016 election occurred in September of 2015 when the FBI contacted the Democratic National Committee’s help desk and left a message to inform them that at least one DNC computer had been compromised by Russian hackers. This outsourced IT technician listened to the message, scanned the network and found nothing. He did not return the FBI’s call or relay the content of it to DNC leadership. The breach was later revealed to be extensive, with hackers gaining access to numerous emails, documents, and communications. In November 2015, the FBI called to inform the DNC that one of their computers was now transmitting information back to Russia. This information still did not make its way to DNC leadership and hackers roamed inside the DNC’s computers for months. It is expected the Russian Military Intelligence service (GRU) – through two Russian intelligence groups called APT 28 (Fancy Bear) and APT29 (Cozy Bear) – had access to the DNC’s computer network from July 2015 to June 2016. Information the GRU accessed began being leaked through the Guccifer 2.0 persona in June and WikiLeaks in July.

In January 2017, FBI Director James Comey said that Russian hackers successfully breached some Republican groups and outdated Republican National Committee systems, but that the hackers did not release this correspondence.

On March 19, 2016, Hillary for America campaign chairman John Podesta received a phishing email ostensibly from Gmail claiming another person had tried to access his account and prompting him to reset his password. Podesta forwarded the email to the campaign’s help desk and a staffer replied with a typo saying the email was “legitimate” – the staffer meant to say
“illegitimate” – prompting Podesta to follow the instructions in the phishing email and unintentionally give Russian hackers access to his inbox.

On October 7, 2016, less than an hour after the Donald Trump and Billy Bush Access Hollywood tape was released to the public, WikiLeaks tweeted that they had 50,000 of John Podesta’s emails and leaked 2,000. Throughout October and November of 2016, WikiLeaks published over 58,000 messages from John Podesta’s account.

The Mueller Report (formally titled Report on the Investigation into Russian Interference in the 2016 Presidential Election) concluded that the Russian Internet Research Agency (IRA) ran social media campaigns “designed to provoke and amplify political and social discord in the United States,” favoring Trump and Sanders and disfavoring Clinton. The IRA has been described as a troll-farm and is funded by a Russian oligarch with ties to Vladimir Putin. A variety of platforms, including Facebook, Instagram, Twitter, Reddit, Tumbler, Pinterest, Medium, YouTube, Vine, and Google+ were used. It is estimated that the IRA purchased $100,000 in Facebook ads through 500 different accounts. Facebook ads purchased by Russian operatives reached an approximated 10 million people. That said, when taking into consideration organic (non paid) content and sharing, Facebook estimated 126 million Americans may have seen posts that originated from Russian operatives. 25% of ads from the IRA were geographically targeted, and these included ads targeted to states like Michigan and Wisconsin, which President Trump won narrowly. Several people associated with the Trump campaign including Donald J. Trump Jr., Eric Trump, Kellyanne Conway, Michael T. Flynn, and Brad Parscale linked to or shared content that originated from an IRA Twitter account. The IRA focused their propaganda campaigns on certain categories of Americans. Black Americans, historically a Democratic voting block, were the most targeted, as Russians attempted to deepen racial divides in the United States. Other IRA content focused on “Muslim or Christian culture, Texas culture, and even LGBTQ culture,” also seeking to deepen existing divisions.

According to the Senate Intelligence Committee, there is no evidence that Russians hacked into voting machines and changed votes in the 2016 election. That said, they concluded that “Russian cyber actors were in a position to delete or change voter data” in the Illinois voter base, but found no evidence that this was done. Furthermore, the Russian government coordinated a spear-phishing attack on at least one U.S. voting software supplier and successfully gained access to at least one email account, according to a leaked NSA memo. Shortly before the election, the Russian military operation sent spear-phishing emails to over 100 local election officials in the United States. Finally, Russian hackers also successfully accessed Illinois and Arizona voter files.

2018 Midterm Elections

According to a report from Director of National Intelligence Dan Coats, in 2018 there was no evidence that voting machines were hacked, though social media misinformation campaigns continued.
Looking Forward: The 2020 Presidential Election

There exists little doubt that foreign actors will attempt to interfere in the 2020 election in the United States. In fact, there is much evidence that attempted hacking and misinformation operations are currently operating with full force. The New York Times and the Brennan Center have covered these efforts and how they’ve evolved. The Russians and other nefarious actors have gotten even more sophisticated. “Fancy Bear” – one of the two Russian intelligence units that hacked Democrats in 2016 – has shifted some of its work to U.S. servers. This makes it much harder for the N.S.A. and other U.S. spy agencies to detect hacking, since they’re limited by law to operating abroad. The IRA has also ditched email accounts and moved to encrypted communication tools. Furthermore, they’re trying to circumvent Facebook political ad ban for foreigners by paying Americans to hand over their accounts. Finally, there are concerns about the security of voting machines, the “hodgepodge of new and old technologies” used to tally and report votes, and the previous hacking of back-end systems used to verify voters’ registration status and identities.

Public and Private Responses to the Threat

Since 2016, both private and public actors have taken steps to address election interference. Despite the inherently public nature of elections, private actors have taken the lead on strengthening protections against interference. This section outlines what platforms like Facebook and Twitter have done to avoid a repeat of the 2016 election as well as the actions that federal and state governments have taken. In general, the platforms have opted to focus their efforts on political advertising rather than the more complex issues of disinformation and inflammatory content. Meanwhile, the federal government's inaction on election interference has led to a patchwork environment as states take one-off approaches towards curbing disinformation.

Internet Platform Responses

Much of the blame for cyber-based election interference has fallen on the giant internet platforms that allowed disinformation to spread like wildfire in 2016. Since then, big tech companies like Facebook, Google, and Twitter have spent billions of dollars to prevent election interference, and each of the “Big Three” have created teams dedicated to election interference. Perhaps in an effort to avoid regulation of their digital advertising, they have focused on ads rather than on content-based regulation. However, their responses have not been uniform either in content or in application, and Congress has remained reluctant to impose uniform regulations on the platforms.

Facebook has made substantial investments in addressing election interference. It tripled the size of its safety and security workforce and developed rapid response centers for the 2020 election tasked with monitoring suspicious activity and quickly removing it. Facebook has addressed advertising misinformation by requiring that anyone running political ads submit proof
of U.S. residency. It has also created a publicly searchable advertising database listing who purchased the ad, where it ran, and who it reached. Facebook announced that it would start labeling content created by state-controlled entities, though it has yet to follow through on this promise. The platform has addressed disinformation by partnering with independent fact-checking organizations to identify and flag false or misleading content and has pledged to remove deepfakes. It claims that it has worked more closely with law enforcement, too.

Facebook points to its identification and removal of fake accounts and content as evidence of its success, but several recent events show the shortcomings of Facebook’s response. Facebook has refused to fact-check political ads or to remove false advertising on its platform. During the 2020 Democratic Primary, Senator Elizabeth Warren purchased and ran an intentionally false political ad in an effort to push the platform to address misinformation in advertising in the 2020 election. The Biden campaign pushed Facebook to remove an ad falsely claiming that Mr. Biden had acted corruptly in Ukraine – an ad that several broadcast networks declined to run. More recently, despite committing to address misinformation during the COVID-19 crisis, as recently as last week (with 50,000 dead from COVID-19), Facebook still made it possible for advertisers to target users based on their “interest in pseudoscience.” And while Facebook has provided some data to researchers, the data is limited and inconsistent in quality – and many researchers claim that its hesitance to turn over data is sidetracking research into election interference.

Twitter has acted aggressively to address advertising-based disinformation on its platform. In late 2019, Twitter announced it would ban all political ads from the site. The platform will still allow issue ads, though it will limit microtargeting for them. The platform has moved to address misleading content more broadly, including by labeling tweets that it views as “deceptive or misleading” by providing “expert context” explaining why the content isn’t trustworthy. It has also instituted new guidelines requiring the labeling or removal of deceptively edited videos. Twitter has also stated that, rather than removing all misinformation, it will promote information from trustworthy sources more aggressively. Twitter has notified users who have interacted with false content from state-owned media, including nearly 700,000 users who interacted with IRA-backed propaganda, and released the tweets to academics. However, Twitter will not remove the accounts of political figures who violate its rules against violent speech and will only take action if the account threatens a particular individual or promotes terrorism or self-harm.

Google has instituted policies to address foreign disinformation and increase advertising transparency, but again, has largely focused on political advertisements. As with Facebook, Google has addressed misleading political advertising by setting up a searchable database of political advertisements – although the database appears not to capture many ads, including those of presidential and congressional candidates of both U.S. parties. Google also has a policy against showing political advertisements in Gmail, but that, too, has failed to filter out candidates’ purchases. Google has stated it will restrict advertisers’ ability to microtarget political advertisements to particular subgroups of users as well, only allowing them to be
targeted at the age, gender, and zip code level. YouTube, one of Google’s subsidiaries, has updated its recommendation algorithm to avoid promoting conspiracies and false information following evidence that it promoted conspiracies and false content. The video platform also labels state-funded and state-controlled media.

Government Responses

The federal response to election interference in the wake of the 2016 election has been lacking. This is partially because the federal government has traditionally delegated election operations to states and municipalities. But under the Trump administration, this deference has turned to abdication. The Trump White House has refused to take substantial steps on election cybersecurity, which is a “taboo” issue in the Trump administration. The first-ever director of national cybersecurity preparedness resigned. However, the FBI, DHS, and NSA have all continued to monitor for foreign interference.

In the tail end of the Obama presidency, state officials agreed to designate election infrastructure as critical infrastructure. However, state election infrastructure itself is outdated: an 11-year-old was able to hack into a model of Florida’s state election website and change votes in less than 10 minutes flat. In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was established within DHS, but its efficacy has been hampered by DHS’s focus on other priorities.

Congress’ efforts to respond to election interference have been meager at best. Over 40 bills aimed at addressing election security languish in the Senate. While Congress finally approved roughly $250 million in state election security funding, experts say this falls dramatically short of what’s needed – an estimated $2.2 billion over 5 years. Moreover, Congress has not provided any guidelines on how that funding is to be spent.

States, left with federal inaction and minimal guidance, have begun to take efforts into their own hands, leading to a patchwork regulatory environment for what is ultimately a national problem. For example, Maryland adopted transparency requirements for online political advertising. California and New York have adopted laws requiring social media companies to maintain all ads in a publicly accessible advertisement archive that contains information on who paid for the ad, the amount spent, and background information on the purchaser’s identity. Each additional effort by a state, however, raises the floor for tech platforms and pushes them to adapt, making it a more effective solution than it might initially appear.

Proposed Reforms

As outlined above, the responses to election interference in the digital sphere have, to date, been piecemeal and fragmented. Private sector efforts vary in tactics and efficacy, with the platforms taking different approaches to preventing disinformation campaigns that miss the broader disinformation problem. The lack of a coherent federal response to election interference has left the brunt of the public sector response on the states, leading to a similarly disjointed and inconsistent regulatory framework. A comprehensive framework to address election interference...
is essential to ensure the integrity of the 2020 elections. There are seven principles that should guide reform efforts:

Making election interference a federal priority
The White House should adopt an unambiguous policy addressing election interference, establishing that cyberattacks will be countered with retaliation in the form of sanctions and diplomatic isolation – and possibly counterattacks. The White House can ensure that this is substantive and message the high degree of prioritization by appointing a cybersecurity representative on the NSC. The representative and DHS’ Cybersecurity and Infrastructure Security Agency (CISA) would be tasked with working with states and localities to protect voting and communicating with the public on the status of election interference.

Establishing federal standards for federal elections and infrastructure
To address the patchwork nature of election security, Congress should establish a uniform set of election standards to protect voter registration and election infrastructure. Congress should resource states to upgrade their election infrastructure by fully resourcing not only election security but also election administration.

Upgrading critical election infrastructure
While some states have made progress in shoring up their electoral infrastructure, many voting machines are so outdated that they pose a security risk ahead of the 2020 election. Congress ought to provide states with adequate funding to replace aging equipment. States also should upgrade the security surrounding their voter registration databases to avoid mass disenfranchisement.

Combating state-sponsored election interference
The U.S. could add teeth to efforts to combat foreign agents’ interference by enforcing the Foreign Agents Registration Act (FARA), which is woefully relaxed and relies on voluntary compliance. Congress could pass legislation requiring media organizations registered under FARA (Russia Today/RT America, Sputnik) to present disclaimers showing their registration as a foreign agent (e.g., having an “Agent of the Russian Government” banner at the bottom of their posts and images). This could apply to both the agent and the provider/platform distributing the content. The breadth of FARA (which was passed during World War II to target fascist and communist propaganda) could raise potential First Amendment concerns, as RT has written. Recent scholarship suggests that provisions are on their strongest ground when targeting those clearly acting under the control of foreign governments (as in the examples of Russian propaganda) and when the activity involves democratic processes, like electioneering (as is the case with election interference).

Working with allies to address election interference
The U.S. should focus on international cooperation in addressing interference, because it is an international issue that is a top priority for many of the United States’ allies. At a minimum, the U.S. intelligence community should cooperate with allies on election cyber threats and establish joint principles on election cybersecurity. The U.S. could also take the lead in setting up the new NATO Cyberspace Operations Center and establish international norms to prevent election interference, deter the use of disinformation and hacked materials, and lead international advocacy against foreign interference through disinformation.

Regulating online political advertising by foreign actors
Greater disclosure and disclaimer requirements targeted towards revealing the true source of the content would increase transparency around foreign interference efforts. Restrictions on foreign spending would also get at the issue. The requirements put in place to address interference should be established by a public body, like the FEC, rather than individual platforms. The disclosure requirements ought to cover targeting information as well to understand which individuals actors are trying to target.

Regulating social media platforms to combat the spread of disinformation
Platforms were the locus of many of 2016’s election interference efforts. Congress should develop a consistent regulatory framework to address the spread of disinformation and protect users’ private information. Platforms should have to identify and clearly label content that is created and promoted by state agents, and notify users when they are affected by disinformation campaigns. They could also make it harder to create anonymous or fraudulent accounts, actively label and/or remove bots, or require verification before content-sharing. They should provide greater algorithmic accountability by telling users more information about why they see what they see, and allow users greater control over that exposure, too. Platforms should have to share information with researchers and academics, while following data privacy restrictions – perhaps by providing open and consistent API to researchers.

Suggested Readings:
CNN, Timeline of Presidential Campaign Hacking in 2016
Special Counsel Robert S. Mueller, III, Report On The Investigation Into Russian Interference In The 2016 Presidential Election
Stanford Cyber Policy Center, Securing Our Cyber Future: Innovative Approaches to Digital Threats
Brennan Center, Securing Elections from Foreign Interference
Rolling Stone, Hackers Are Coming for the 2020 Election and We’re Not Prepared
Elizabeth Warren, Fighting Digital Disinformation