Election Interference: An Evolving Strategic Situation

Andrew Rose

POLS 290-001W

Political Science Capstone

Fall 2020 Semester

Introduction

While democratic government is a commonplace geopolitical model today, there are still some states dedicated to the erosion of democratic values. Perhaps there is no pillar more integral to a functioning democracy than free elections. One of the best ways to compromise that foundation is through election interference. This practice, which can involve cyber-attacks on a variety of targets, the dispersal of 'fake news' and the co-option of stateside actors, has recently become a topic of much discussion. It is, in fact, too far ranging a concept to tackle in one place. The many disparate appearances which interference takes on, as well as its many potential trajectories complicate any study of the matter. A completely comprehensive survey will not be undertaken here.

Firstly, what exactly election interference is must be defined. The exactness is what makes this a demanding task. When it is accomplished, it should be clear what harm interference can really do. The next point of exploration is one that becomes increasingly complex depending upon one's worldview and political affiliation: what can be done about it?

As a destabilizing tool, election interference has been deployed with increasing dexterity by numerous international actors. While most modern states have offensive and defensive cyber tools in their arsenals, there are only a select handful which use cyber meddling to interfere in elections and other democratic processes. China, North Korea and Iran all engage in cyber meddling and election interference, although with sometimes diverging methods and disparate goals in mind.

It should be stated clearly that despite the plethora of cyber tools common to interference, not all interference is perpetrated via cyber means and there are many offensive cyber

capabilities which do not constitute election interference. This review will not detail all cyber-operations, but it will attempt to clarify the extent of interference and its body of tactics. As it is a rapidly ballooning field of research, only Russia's efforts will be discussed at length here. Interference typically has three kinds of outcomes, these being 1) to manipulate votes 2) to manipulate voters and 3) to undermine voter confidence; while no U.S. votes have ever been directly manipulated (as far as we can observe) the tandem goals of manipulating voters and undermining voter confidence have certainly been met.

Targeted states cannot wholly neutralize sustained efforts at interference but there is a wide array of mitigating strategies that has proven successful. These strategies (for the sake of brevity, only Canada's response will be summarized here) when compared with the strategic response of the U.S. may reveal strengths as well as weaknesses in our defense against election interference. The evolving strategic threat of foreign interference requires an evolved defensive strategy if the threat is to be effectively mitigated.

Russian Strategy

Information manipulation has always been a tactic of authoritarian regimes and illiberal governments. Ever since the advent of the printing press, unscrupulous statesmen have sought to exercise control over the various narratives consumed by their people. Every revolution in information and communication technology—from the invention of the telegraph to the first computers—has altered the art of information manipulation. The creation of the internet was no different. Even as society wavers on the cusp of the Artificial Intelligence (AI) era, there remains a significant struggle to understand the penetrating influence of the world wide web. While its virtues are undeniable, its dark potentialities have become more and more troubling with time.

Perhaps there is no regime more well-equipped to comprehend these dark potentialities than Russia and no statesman living more unscrupulous than Vladimir Putin.

Putin's strategy of covert information warfare is founded on the Gerasimov Doctrine, named for the Chief of the General Staff (Russian Armed Forces), General Valery Gerasimov. His Doctrine, which calls for a kind of 'hybrid warfare' involving cyber capabilities and propaganda, remains a government-wide policy even in peacetime. This doctrine is couched in a larger foreign policy doctrine named after Yevgeny Primakov. Students of Russian history will recognize Primakov not only as a powerful politician and diplomat but also as the man who oversaw the KGB's near-seamless transition into the SVR (Foreign Intelligence Service). The Primakov Doctrine calls for Russian supremacy in the post-Soviet sphere of influence and a strong oppositional stance towards both U.S. power and the expansion of NATO.[1]

A report from the Center for a New American Security explains how Russia has always, at least in its two most recent iterations, been quick to acquaint itself with new manipulation tactics and capabilities:

> "While propaganda has long been a part of the Kremlin's arsenal—playing a prominent role throughout the Cold War—Russia's conflict with Georgia in 2008 marked an important turning point in the Kremlin's use of information warfare. The Kremlin perceived that Russia lost the battle over the narrative of events in Georgia, underscoring for Moscow the importance of being able to advance Russia's worldview."[2]

The Georgian-Russian War, despite its brevity, was the first time cyber capabilities were used in a context of warfare.[3] After a swift victory and a negotiated ceasefire Russian troops continued to occupy Russian speaking sectors of Georgia, disregarding the terms of the ceasefire.[4] Despite

[1]Rumer, Eugene. *"The Primakov (Not Gerasimov) Doctrine in Action."*
[2]Fitt, Joshua et al. *"Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations."*
[3]Beehner, Lionel et al. *"Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia."*
[4]*"Clinton Slams Russian 'Occupation' of Disputed Enclaves on Georgia Visit."*

being able to claim victory the Kremlin felt that their control of international perceptions, especially online, was compromised and immediately set about improving Russia's information warfare capabilities.

The reader may recall that Russia has since gone on to annex another bordering territory (in the Crimea) after a very similar but more efficient campaign.[5] The evolving information landscape of the 21st Century, brought about in part by the internet, has convinced many states—Russia chief among them—to manipulate not only their own populations, but also diaspora communities and foreign citizens of adversarial states. Russia has the overarching strategy to justify interference, it has practical experience and no qualms about interfering. So, what does modern election interference really look like?

Russian Interference Tactics

As has been noted, there are three broad kinds of outcomes typically sought when interfering in a target state's elections or other democratic processes. At the risk of being repetitive they are to 1) manipulate votes 2) manipulate voters and 3) to undermine voter confidence. Each outcome typically involves multiple tactics and there are many tactics which may contribute to the success of multiple outcomes.

While Russia has successfully manipulated online vote counts in the past (2014 Ukrainian Presidential Election) there is no evidence that they have attempted this when interfering in U.S. elections.[6] One may wonder why, since tech conferences have shown that many voting machines currently in use in the U.S. can be compromised by even inexperienced

[5]Polityuk, Pavel and Zawadzki, Sabina. *"Ukraine Says Russia Follows Pre-Georgia War Scenario in Crimea."*
[6]Ee, Shaun and Galante, Laura. *"Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents."*

hackers with relative ease. For one, this kind of security breach would constitute a significant escalation—an explicit violation of international law on Russia's part.[7] Perhaps it is also partly because Russia has found so much success in achieving the other two outcomes by exploiting existing social divisions and sowing doubt via relatively weak platform infrastructures and willing stateside actors. It should be mentioned that while official vote tallies have not been compromised, voter rolls and official election websites have been successfully targeted before.

Since as early as 2014 the Kremlin has pumped money, disinformation and inflammatory rhetoric into nearly every social media platform via state-controlled media outlets, troll-farms and shadow organizations. Some favored tactics are to play up racial divisions, spread conspiracy theories and to organize mutually antagonistic protests. All these tactics are designed to serve an overarching strategy. That is, to sow confusion and undermine faith in the democratic system. Most states witnessed attempted hacks of their electoral systems in 2016. Internal documents from Hillary Clinton's campaign were successfully hacked and published. The DNC also had internal documents published in the run-up to the election.[8] Those committing acts of interference are often peripheral actors whose links to the Russian state can be challenging to confirm. Most clues, however, point either directly or indirectly to the influence of the Kremlin and other Russian intelligence/security ministries.

One episode from the 2016 presidential election obscured the then-emerging issue of interference. On July 27th, candidate Donald Trump appeared to plead directly to Russia while he addressed a crowd at a campaign event in Florida. Looking into the camera, he said "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing" (referencing

[7]Hern, Alex. *"Kids at hacking conference show how easily US elections could be sabotaged."*
[8]Ee, Shaun and Galante, Laura. *"Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents."*

deleted emails from Hillary Clinton's private server). Later that day, operatives of GRU (Russia's Main Intelligence Directorate) attempted to hack email accounts connected with Clinton's personal office.[9] Whether or not a candidate publicly asks for foreign interference, the public appearance of doing so—sarcastic or not—serves to cloud the real danger posed by interference.

Kremlin-backed operations learned a lot from 2016. While the overall strategy remains largely the same, tactics have shifted to provide even more deniability. According to a 2019 report from the Center for Strategic and International Studies (CSIS), "Russia has reduced original content creation in favor of amplifying authentic U.S. voices online to better obfuscate the extent of their interference."[10] It has become increasingly apparent that there are a multitude of 'authentic U.S. voices' that are all too eager to echo the propaganda and intentionally divisive rhetoric peddled by the Kremlin. Which of these voices are conscious of their alignment remains troublingly unclear.

Another disconcerting development can be found in the rising popularity of artificial intelligence as a weapon for waging information warfare. 'Deep-fakes' (altered video content which can convince the undiscerning eye) have swarmed social media platforms with misleading material for a few years now. Advances in AI have made the production of deep-fakes a much easier task, and the technology has become obtainable far and wide.[11]

All the tactics employed by Russia have been relatively subtle, but they have also posed real threats to the smooth continuation of the democratic process and the sway of democratic

[9]Day, Chad and Tucker, Eric. *"Mueller Revealed His Trump-Russia Story in Plain View."*
[10]Nair, Devi et al. *"Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System."*
[11]Villasenor, John. *"Deepfakes, Social Media, and the 2020 Election."*

values. In 2020, Russia's playbook for interference expanded upon proven tactics and introduced unfamiliar tactics. They're overarching strategy remains the same but the means to implement that desired end are evolving right alongside the information landscape.

U.S. in the Wake of 2016 Interference

Ever since the facts of foreign election interference became clear to the public, the issue has become a cultural flashpoint and, in many ways, a partisan slugfest. During the 2016 election, Senate Majority Leader Mitch McConnell initially declined to cooperate with the White House when it came to publicizing the facts of interference. Nearly out of options, President Obama confronted Vladimir Putin privately at a summit. As a last resort, a public statement on Russian Interference was released in October, rather late in the campaign season. In December of 2016, several Russian diplomats, accused of spying, were expelled and their facilities were seized. Numerous punitive sanctions were also levelled by the Obama administration before the transition of power.[12]

After the election was over, many Republicans were quick to claim that Russian election interference had not been significant enough to influence the results. Conversely, many Democrats quickly seized upon initial findings in order to question the legitimacy of Trump's election to the presidency.[13] Meanwhile, Russia denied all accusations of interference. At this point, the definitions of interference were nowhere near cohesive and the timeline of events was still far from comprehensive. A self-published report from 2020 detailing case studies of foreign interference in Asia made this clarification: "…because accusations of foreign interference often…have political implications and evidence is often murky, nations who are accused of

[12]Ewing, Phillip. *"Fact Check: Did The Obama Administration Respond To Election Interference By Russia?"*
[13]*"The Republicans' Defensiveness about Russian Hacking Is Revealing."*

foreign interference, as well as domestic actors who have been accused of being complicit in foreign interference, often contend that they have been wrongly accused."[14] Sufficient evidence is paramount when levelling accusations and denials of wrongdoing are, by no means, sufficient evidence for exoneration.

In 2017, not long after the Director of the FBI (James Comey) was fired, the Department of Justice appointed a special counsel to oversee an investigation into Russian interference in the 2016 election. There were reports that the President was stopped, by his own subordinates, from ending the investigation prematurely. In March of 2019 the LA Times reported that "Mueller and his team ultimately charged 34 individuals, including 25 Russians. Seven people pleaded guilty, including several in Trump's inner orbit."[15] The former President's willingness to pardon his associates and/or downplay their convictions did not help to ease confusion or division around the issue.

Aside from dozens of indictments and numerous follow-up investigations, the final report produced by the special counsel detailed some of the Russian interference operations that transpired either during 2016, or in the few years prior. The American Constitution Society provided this bullet point analysis of the special counsel's election interference findings:

- Russian interference in the 2016 election was "sweeping and systemic."
- Major attack avenues included a social media "information warfare" campaign that "favored" candidate Trump and the hacking of Clinton campaign-related databases and release of stolen materials through Russian-created entities and Wikileaks.
- Russia also targeted databases in many states related to administering elections gaining access to information for millions of registered voters.[16]

[14]Ang, Benjamin et al. *"Cases of Foreign Interference in Asia."*
[15]Mergerian, Chris and Wilber, Del Quentin. *"Mueller submits Trump-Russia investigation report but doesn't recommend additional indictments."*
[16]*"Key Findings of the Mueller Report: ACS."*

While the special counsel did not indict any American citizens for conspiracy or collusion, the findings specified that the President could not be exonerated from the charges of obstruction of justice. The President's attempts to shut down the investigation had become a central pillar of the investigation.[17]

A Divided Response

As has been hinted at, there was much disagreement as to how to respond to the new strategic threat presented by election interference. As has been alluded to above, the President's finances and ties to Russia, as well as his uncouth behavior during the campaign, came under intense and immediate scrutiny. Support for the President, as he deflected allegations and prompted investigations, fell mostly along party lines. This partisan dispute is still a feature of the ongoing debate around interference and deterrence.

A 2017 report from the Air University Press sums up the position of the U.S. (at the time) in regards to interference rather nicely: "Current US strategy falls short on several key attributes necessary for effective deterrence…deterrence by denial is a passive strategy—and insufficient on its own to achieve cyber deterrence."[18] Denial of any sort, whether it be wholesale or piecemeal, ultimately compromises efforts at real deterrence. Denial will not just muddle strategies for cyber deterrence. It actively hinders most of the mitigating strategies for deterring future interference.

Most actors, however, did not retreat to outright denial and both sides came to agree on certain points, such as levelling sanctions, holding social media platforms to account and

[17]Office of the Special Counsel. *"Report On The Investigation Into Russian Interference In The 2016 Presidential Election."*
[18]McKenzie, Timothy. *"Is Cyber Deterrence Possible?"*

increasing federal funding for voting infrastructure. Significant discord arises when the severity of sanctions, the correct way to hold platforms accountable and/or the amount of funding are debated.

While President Trump initially approved sanctions on Russian individuals and organizations, his administration drew bipartisan criticism from both houses of Congress for lifting sanctions on Oleg Deripaska (an oligarch with ties to Vladimir Putin & Paul Manafort) in 2019.[19] Democrats on the hill found the rationalizations of the Treasury Department (which oversees the implementation of sanctions) unconvincing and criticized any show of leniency towards the shadowy billionaire.[20] Lifting sanctions—that have been placed in retaliation for interference—inevitably colors the responsive strategy as inconsistent.

Republicans have consistently disagreed with Democrats about how exactly to hold social media companies to account. Tech and media giants, including officers representing Facebook, Twitter and more recently Google, have testified before Senate committees multiple times since 2016. They've been grilled on their ability to combat fake news as well as their methods therein and the transparency of those methods. While Democrats have largely insisted on greater transparency for advertising policies and more fact-checking, Republicans have echoed the President, claiming that internet platforms 'censor' conservative voices more than others.[21] Voices from either party strongly support reforming Section 230, which governs internet platform liability. Reforms look completely different depending upon the side one finds

[19]Desiderio, Andrew. *"House rebukes Trump for easing Russia sanctions."*
[20]Rappeport, Alan and Fandos, Nicholas. *"Mnuchin Defends Plan to Lift Sanctions on Russian Oligarch's Companies."*
[21]Guynn, Jessica. *"Trump-Led Conservatives Accuse Big Tech of Election Interference, Escalate Bias Charges Ahead of Senate Showdown."*

themselves aligned with. The former President also voiced significant frustration with Section 230 while he held office.[22]

Both parties more-or-less agree on increasing funding for voting infrastructure, but disagreements tend to center on the amount and priority of funding. In 2016, there hadn't been federal funding allocated for election upgrades/security since HAVA (Help America Vote Act, 2002).[23] Several bipartisan bills dealing with election security were introduced in Congress from 2017-2019. Most of those bills have not cleared both chambers.[24] In 2019 Congress appropriated $380 million for the U.S. Election Assistance Commission to disburse to the states and passed the DETER Act which denied visas for election meddlers.[25] Federal funding of elections remains a point of legislative contention.

Despite some important compromises being made in the past four years, disagreements seem to have weighed more heavily on public opinion. In 2020, Pew Research found that "Americans have become less confident that the federal government is making serious efforts to protect U.S. elections from hacking and other technological threats. Since October 2018, the share of Americans who say this has declined from 55% to 47%."[26] As the threat persists and waxes in strength, many political leaders complicate matters, and more and more people are losing confidence in the response to interference.

Traditional & Social Media Response

[22]Brown, Abram. *"What Is Section 230-And Why Does Trump Want To Change It?"*
[23]*"Help America Vote Act: U.S. Election Assistance Commission."*
[24]Fandos, Nicholas. *"New Election Security Bills Face a One-Man Roadblock: Mitch McConnell."*
[25]Martinez, Gabriela. *"How the U.S. is trying to improve election security ahead of 2020."*
[26]Hartig, Hannah. *"Poll: 75% of Americans say it's likely that Russia or other governments will try to influence 2020 election."*

It is plain to see that media outlets, regardless of medium, have an integral role to play in combating election interference. A 2020 report from CSIS concerning Russian and Chinese interference came to this conclusion: "A vibrant free press has proven to be critical…in exposing the full extent of malign interference activities by foreign authoritarian governments and launching national debates around how to best respond…Democracies with high trust in traditional media appear less vulnerable to information manipulation…"[27] While President Trump is inclined to inhabit and influence the airwaves, he and his slew of press secretaries frequently labeled critical and objective press stories as 'fake news.' Does this reflect a distrust of traditional media or has trust been purposely eroded? Or perhaps both?

Social media is a relatively new occurrence in the information landscape. It seems safe to say that much misinformation and disinformation (information which is accidentally misleading or purposely misleading), whether originating from foreign sources or being amplified by them, appears on such platforms. Because social media was not originally conceived of as an alternative source of news, the reckoning has been labored and slow moving. Much has been made of increased congressional oversight and various internal changes, but many question the sincerity and efficacy of these incremental shifts. A 2020 report from New America summarized the state of things like this:

> "Since 2016, internet platforms have instituted a range of policies and practices that seek to identify and curb the spread of election-related misinformation and disinformation. However, experts and users have little confidence in the efficacy of these measures…there is still a significant lack of transparency around how these platforms are creating and implementing these policies, sparking concerns that these policies are not being implemented consistently and are ineffective. In addition, this has also raised

[27]Conley, Heather A. et al. *"Countering Russian and Chinese Influence Activities: Examining Democratic Vulnerabilities and Building Resiliency."*

> concerns that platforms may be prioritizing profit over the safeguarding of user rights and the electoral process."[28]

Platforms that have banned political advertising outright would almost certainly deny that they are prioritizing profit, yet it can be questioned whether their approach is helpful to the larger situation or merely helpful in limiting their own liability.

While there is no question that platforms have stepped up their efforts to clamp down on manipulated information, there remain glaring and manifold loopholes even among the most powerful players. A recent example of one of these loopholes was detailed in an NPR article by Shannon Bond:

> "Facebook…users shared a screenshot of a tweet claiming, falsely, that President Trump was deliberately infected with COVID-19 by "the left." Facebook overlaid a warning label on some versions of the post, saying independent fact-checkers determined it was "false information," and linking to a USA Today article debunking the claim.
>
> But Facebook did not apply the same label to versions of the message that were nearly identical, except with different backgrounds or croppings…
>
> …nearly 42% [of misleading posts], were not labeled, even though they contained claims that had been debunked."[29]

Even as Mr. Zuckerberg and other internet moguls defend the capacity of their platforms to combat fake news—even as their efforts have been doubled and apparently redoubled—manipulated (and often malicious) information still manages to find a welcoming home on a platform meant to foster networking. These platforms do just that on a scale that used to be unimaginable.

Voting Infrastructure & Civil Society

[28]Blasé, Margerite and Singh, Spandana. *"Protecting the Vote: How Internet Platforms Are Addressing Election and Voter Suppression-Related Misinformation and Disinformation."*
[29]Bond, Shannon. *"Tiny Changes Let False Claims About COVID-19, Voting Evade Facebook Fact Checks."*

Another considerable obstacle to mitigating the effects of interference is improving voting infrastructure. The administration of U.S. elections, including federal elections, is left up to the states. While some states have uniform voting systems and updated voting technology, others have patchwork voting systems and outdated voting technology. According to a 2019 analysis by the Brennan Center for Justice, there were at least eight states that would still have paperless balloting in 2020. That same analysis also noted that many states still do not mandate post-election audits before certification of results.[30] While these gaps in the system do not necessarily jeopardize the overall security of elections, they do lend themselves somewhat to popular doubts about the integrity of the process.

One major hurdle to improving infrastructure is the absence of concerted leadership. as Kamarck and West point out in their book, Dirty Tricks in the Digital Age: "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."[31] For instance, in August then-President Trump threatened to sabotage funding for mail-in balloting (something integral to voting infrastructure, especially mid-pandemic) before recharacterizing his statements.[32] He continues to claim, on a related note and without evidence, that there are vast infrastructural loopholes which allowed for widespread voter fraud to occur in the 2020 presidential election.[33] Such posturing renders the improvement of infrastructure a needlessly fraught process.

---

[30]Howard, Elizabeth et al. *"Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary."*
[31]Kamarck, Elaine and West, Darrel. *"Dirty Tricks in the Digital Age."*
[32]Khan, Miriam. *"Trump suggests he'd oppose USPS funding to hurt mail-in voting, then says he won't."*
[33]Herman, Steve. *"Trump, Without Evidence, Makes Vote Fraud Claims."*

When the head of Cybersecurity and Infrastructure Security Agency (CISA), a non-partisan official tasked with securing elections, confirmed the security of voting infrastructure in a joint statement, he was fired for making supposedly inaccurate statements.[34] According to a contemporaneous PolitiFact fact-check no "substantial or coherent" evidence was provided by the Trump Administration as to how the CISA statement was inaccurate.[35] There are not a few improvements to be made before the effects of interference can be allayed, but suggesting the entire system is rotten to the core, without a substantial foundation, serves to complicate efforts at structural upkeep and borders on actual interference, albeit of a domestic flavor.

A productive strategy to counter election meddling includes the forceful rebuttal of misinformation and disinformation about voting infrastructure. For a rebuttal to be potent, it must be delivered in a coordinated and cooperative fashion. Even a single voice of contradiction will undermine the effect of the rebuttal. As a report from the Army Cyber Institute makes clear, a fruitful response to election meddling requires significant levels of coordination, not only within government, but also with private parties and elements of civil society:

> "If states aim to reduce their vulnerabilities and contrast cyber threats such as cyber election meddling…The identification of further preventive efforts, in terms of strengthening cyber defense capabilities to protect electoral processes, is a topic that merits further discussion…states have to think in terms of integrated strategies which cannot avoid the involvement of international law, but, at the same time, must require the active intervention of other disciplines."[36]

While much of American civil society (i.e. institutions of education, advocacy and business) has responded to the need for a coordinated rebuttal, not all relevant players are willing to cooperate. Efforts to integrate strategies across the board are all too easily hamstringed by vocal dissent.

---

[34]Brangham, William and Norris, Courtney. *"Why Trump fired the official charged with securing U.S. elections."*
[35]Noah Y. Kim. *"Fact-checking Donald Trump's tweet firing Christopher Krebs."*
[36]Rotondo, Annachiara and Salvati, Pierluigi. *"Fake News, (Dis)information, and the Principle of Nonintervention: Scope, limits, and possible responses to cyber election interference in times of competition."*

The internet moguls are changing their approaches measure by measure, yet the information landscape may change quicker. Institutions of education and research have shed light on the topic (perhaps it has never been so well lit) and yet the very meaning of 'fake news' remains a matter of public controversy. Technological advancements provide for greater coordination and a more meaningful rebuttal in terms of cyber defense and safeguarding infrastructure, and yet these gains may be ultimately inconsequential. U.S. civil society has its fair share of interference disavowers/enablers and such attitudes even seem to have taken entire portions of the federal government hostage for a time (*sans* the intel community). The dissent within civil society would likely not be as meaningful if there were not viewpoints within government to lend them legitimacy. Can the words and actions of leaders really undercut the success of a cooperative response?

Leadership in a Coordinated Response

One essential factor of coordinating to prevent foreign interference (and mitigate its effects) is clear and consistent leadership. Has this outcome proved evasive or attainable? Another excerpt from Dirty Tricks in the Digital Age reads: "From the very beginning of his presidency, Donald Trump has denied or downplayed Russian interference in the 2016 presidential campaign. He has at various times dismissed the entire 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."[37] Said declarations of innocence recall the elaboration on accused domestic actors mentioned in the Case Studies of Foreign Interference in Asia (pg. 8). Consider the Trump Administration's near-categorical dismissal of

[37]Kamarck, Elaine and West, Darrel. *"Dirty Tricks in the Digital Age."*

Russian interference reporting in contrast to their selective amplification of Chinese Interference news (detailed on pgs. 17, 18). A consistent leadership approach in combating foreign interference seems to have been a rather evasive proposition in 2020.

A thematic brief on the congressional investigations of Donald Trump from the think tank Third Way confirms the complicating patterns displayed by the President:

> "President Trump's governing style deviates dramatically from the approaches followed by his predecessors. His propensity to ask for foreign interference in American Elections, lack of transparency, erratic decision making, political retaliation and potential self-dealing has led to over 300 House congressional hearings and more than 900 oversight letters into his actions. It has also resulted in federal criminal investigations into Trump associates, and criminal and civil investigations in New York state, where the Trump Organization is headquartered…While Republicans have focused their complaints on minor procedural flaws within the investigations, they have been unable to disprove the main allegations against the president: that he sought and accepted assistance from foreign governments for his personal and political benefit, obstructed investigations into those allegations, and been personally self-enriched at the taxpayers' expense."[38]

The former President's reactions to election interference are striking when juxtaposed with the above allegations. He has even availed himself of one of the favored tactics of the Kremlin, that is, to sow doubt about the integrity of elections. Unrealistic doubts expressed by even one leader, especially one so powerful, can place a cloud of uncertainty around a larger issue. This has unavoidable ramifications for any democratic society.

A recent AP-Norc Poll found that most Americans are at least "somewhat concerned" about the possibility of foreign interference in this year's election. Their findings continue:

> "Austin Wright, an assistant professor at the University of Chicago's Harris School, said it was striking that Americans are not more concerned by the threat of foreign interference given the range of dangers. He suggested that may have to do with domestic concerns currently occupying public attention, and with the fact that some American leaders — including Trump — are themselves working to undermine confidence in the election.

[38] *"2020 Thematic Brief: Trump Investigations – Third Way."*

> The August intelligence assessment that outlined ongoing Russian interference also noted that China regards Trump as unpredictable, prefers that he lose to Biden and has been working to shape the U.S. policy environment.
>
> Trump has seized on that finding as he and several other senior administration officials have tried to make the case that Beijing is the more assertive adversary. Trump has repeatedly maintained that China is working to defeat him, though Microsoft noted in a blog post last month that among those targeted by Chinese state-backed hackers are people associated with the Biden campaign."[39]

Campaigns were being targeted by foreign adversaries and at least one candidate actively sowed confusion—it's no wonder most Americans were worried. Is it possible that the top-down proliferation of incertitude has lessened the impact of foreign interference news?

According to an analysis provided by the Washington Post, whistleblower Brian Murphy—a senior DHS official—alleged that he was enjoined by department officials to shift the focus of his assessments of foreign interference to states other than Russia:

> "'In mid-May 2020,' the complaint reads, 'Mr. Wolf instructed Mr. Murphy to cease providing intelligence assessments on the threat of Russian interference in the United States, and instead start reporting on interference activities by China and Iran.' The instructions, Wolf allegedly said, came from Robert C. O'Brien, Trump's top aide on national security…"

The analysis goes on to paraphrase and quote William Evanina, the Director of the National Counterintelligence and Security Center. He added some clarity to Russia ad China's divergent goals and strategies:

> "In early August, more detail was added by Evanina: China actually hoped that Trump would lose the election given his 'unpredictable' nature. China wasn't trying to shape voter outcomes specifically, however, while Russia was.
>
> 'We assess that Russia is using a range of measures to primarily denigrate former vice president Biden and what it sees as an anti-Russia establishment,' Evanina said at the time."[40]

[39]Swanson, Emily and Tucker, Eric. *"Poll: Americans concerned by foreign interference."*
[40]Bump, Phillip. *"Reports about foreign interference in U.S. politics have been useful to Trump's campaign. That may not be an accident."*

Even though the former President and his top administration officials recognized some instances of interference, they muddied the seriousness of the threat and complicated the work that counters it when they cherry picked conclusions.

One of the essential elements of prevention and mitigation is sharing all findings publicly, when deemed necessary. Arbitrarily deeming some findings pertinent and others not, and then publicizing the former before full governmental coordination, is questionable. As the chief executive of the federal government, the president has substantial power to set the standards for the federal response to election interference.

Summary of the Canadian Situation

To put the U.S. response in perspective, let's briefly consider the approach taken by a close neighbor and ally, Canada. After Russia interfered in the federal elections of 2015, Prime Minister Justin Trudeau's government was determined to prepare for a repeat in 2019. Some journalists and conservative politicians questioned why Trudeau's government wasn't more transparent with the details of Russian interference.[41] There are many similarities between the situation of the U.S. and that of Canada with regards to interference. Russia used many of the same tactics in Canada for many of the same reasons they would make use of those tactics a year later in the U.S. While the methods of transparency utilized by the two countries are divergent, the outcomes are similar in the way they produce confusion and consternation.

Canada's response differed from that of the U.S. in many other respects. A 2019 article from Politico confirmed that Canadian measures went further than U.S. measures in exacting transparency on advertising from social media platforms. It also reported "In January 2017,

[41]Bryden, Joan. *"Feds Refuse to Disclose Details of Russian Meddling in Canadian Elections."*

Trudeau appointed Karina Gould to a cabinet position with a new mandate: to work with the intelligence community to protect the election [2019] against cyberattacks…" The article also details the functions of the Critical Election Incident Public Protocol, a project headed by bureaucrats which is supposed to alert "both political parties" as well as the public to foreign interference.

While there are non-partisan bureaucrats tasked with sounding alarms in the U.S., their statements are often misapplied or dismissed for plainly partisan purposes. No cabinet positions or special committees have been created in the U.S. specifically to address the issue of election meddling. Where Canadian leadership tends to defer to its intelligence services and other non-partisan institutions when informing policymakers and the public, U.S. leadership had a habit of suppressing or amplifying specific findings (as mentioned above) for partisan positioning.

A 2020 report detailing the comprehensive Canadian response to interference in their 2019 federal elections contains the following excerpt:

> "The composition of the Canadian House of Commons Special Committee on Electoral Reform was made public online, with brief explainers on the objectives and scope of the Special Committee…(Bill C-76) was introduced to safeguard Canadians' trust in democratic processes and increase public participation in democratic activities…The Canadian government has heavily advocated for greater regulation of social media platforms, leading to greater communication with them, and the platforms have so far been responsive to government concerns. The CSC has also advocated for increased algorithmic transparency by social media companies."[42]

Bill C-76 reformed Canadian elections in several ways. Aside from adjustments aimed at preventing foreign interference, the window for campaigning was shortened and spending limits for campaigns were prescribed. Regulations to restrict campaign spending and to impel the use of a Canadian bank account pertained only to political third parties.[43]

---

[42]Leong, Dymples. *"Securing Elections amd Beyond: Lessons for Singapore from Canada's 2019 federal election."*
[43]Zimonjic, Peter. *"Liberals' Election Reform Bill Becomes Law on Last Day of Parliamentary Sitting."*

Clear and consistent executive leadership, a commitment to reform and a non-partisan approach have successfully safeguarded Canadian elections and faith in democratic values. The withholding approach to governmental transparency, and its effects on Canadian discourse, provide lessons on the importance of forthcoming and consistent transparency.

Conclusion

Free and fair elections are an essential component of the democratic process. Any attempt to interfere with the integrity of the election process poses a strategic threat. As information technology evolves over time, so does the threat. A successful response to interference cannot be 1) mired in partisan debate 2) cannot lack genuine transparency and 3) cannot be uncoordinated or inconsistent. The efficacy of any given response is surely tied to these three things and to its capacity for evolution.

Bibliography

"2020 Thematic Brief: Trump Investigations – Third Way." Third Way, 17 Sept. 2020, www.thirdway.org/primer/2020-thematic-brief-trump-investigations.

Beehner, Lionel, et al. *"Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia."* Modern War Institute at West Point, Modern War Institute , 20 Mar. 2018, mwi.usma.edu/wp-content/uploads/2018/03/Analyzing-the-Russian-Way-of-War.pdf.

Bertrand, Natasha. *"What Mueller Leaves Behind."* The Atlantic, Atlantic Media Company, 26 Mar. 2019, www.theatlantic.com/politics/archive/2019/03/questions-mueller-probe-raised-about-trump/585526/.

Blasé, Margerite and Singh, Spandana. *"Protecting the Vote: How Internet Platforms Are Addressing Election and Voter Suppression-Related Misinformation and Disinformation."* New America, 12 Nov. 2020. doi:10.2307/resrep26363.4.

Brangham, William, and Courtney Norris. *"Why Trump Fired the Official Charged with Securing U.S. Elections."* PBS, Public Broadcasting Service, 18 Nov. 2020, www.pbs.org/newshour/show/trumps-dismissal-of-christopher-krebs-draws-widespread-criticism.

Brown, Abram. *"What Is Section 230-And Why Does Trump Want To Change It?"* Forbes, Forbes Magazine, 29 May 2020, www.forbes.com/sites/abrambrown/2020/05/28/what-is-section-230-and-why-does-trump-want-to-change-it/?sh=43421e11389d.

Bryden, Joan. *"Feds Refuse to Disclose Details of Russian Meddling in Canadian Elections."* CTV News, 22 Nov. 2018, www.ctvnews.ca/politics/feds-refuse-to-disclose-details-of-russian-meddling-in-canadian-elections-1.4188942.

Bump, Philip. *"Analysis | Reports about Foreign Interference in U.S. Politics Have Been Useful to Trump's Campaign. That May Not Be an Accident."* The Washington Post, WP Company, 9 Sept. 2020, www.washingtonpost.com/politics/2020/09/09/reports-about-foreign-interference-us-politics-have-been-useful-trumps-campaign-that-may-not-be-an-accident/.

"Clinton Slams Russian 'Occupation' of Disputed Enclaves on Georgia Visit." France 24, AFP, 5 July 2010, www.france24.com/en/20100705-georgia-occupation-russia-clinton-visit-saakashvili-abkhazia-south-ossetia-ceasefire.

Conley, Heather A., et al. *"Countering Russian and Chinese Influence Activities: Examining Democratic Vulnerabilities and Building Resiliency."* JSTOR, Center for Strategic and International Studies (CSIS), 1 July 2020, www.jstor.org/stable/resrep25322.

Day, Chad, and Eric Tucker. *"Mueller Revealed His Trump-Russia Story in Plain View."* AP NEWS, Associated Press, 22 Mar. 2019, apnews.com/article/3c4bc6e9aa6c4fb18bc9603fb082af65.

Desiderio, Andrew. *"House Rebukes Trump for Easing Russia Sanctions."* Politico, 17 Jan. 2019, www.politico.com/story/2019/01/17/house-rebukes-trump-russia-sanctions-1108939.

Ewing, Philip. *"Fact Check: Did The Obama Administration Respond To Election Interference By Russia?"* NPR, 15 July 2018, www.npr.org/2018/07/15/629281975/fact-check-did-the-obama-administration-respond-to-election-interference-by-russ.

Fandos, Nicholas. *"New Election Security Bills Face a One-Man Roadblock: Mitch McConnell."* The New York Times, 8 June 2019, www.nytimes.com/2019/06/07/us/politics/election-security-mitch-mcconnell.html.

Fitt, Joshua et al. *"Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations."* Center for a New American Security, 2020. 4-5. Accessed November 3, 2020. doi:10.2307/resrep25314.5.

Galante, Laura, and Shaun Ee. *"Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents."* Atlantic Council, 3 Nov. 2018, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents/.

Guynn, Jessica. *"Trump-Led Conservatives Accuse Big Tech of Election Interference, Escalate Bias Charges Ahead of Senate Showdown."* USA Today, Gannett Satellite Information Network, 27 Oct. 2020, www.usatoday.com/story/tech/2020/10/27/facebook-twitter-senate-hearing-republicans-make-censorship-accusations/3750041001/.

Hartig, Hannah. *"Poll: 75% Of Americans Say It's Likely That Russia or Other Governments Will Try to Influence 2020 Election."* Pew Research Center, 27 Aug. 2020, www.pewresearch.org/fact-tank/2020/08/18/75-of-americans-say-its-likely-that-russia-or-other-governments-will-try-to-influence-2020-election/.

"Help America Vote Act: U.S. Election Assistance Commission." Help America Vote Act | U.S. Election Assistance Commission, EAC, www.eac.gov/about_the_eac/help_america_vote_act.aspx.

Herman, Steve. *"Trump, Without Evidence, Makes Vote Fraud Claims."* Voice of America, VOA, 6 Nov. 2020, www.voanews.com/2020-usa-votes/trump-without-evidence-makes-vote-fraud-claims.

Hern, Alex. *"Kids at Hacking Conference Show How Easily US Elections Could Be Sabotaged."* The Guardian, Guardian News and Media, 22 Aug. 2018, www.theguardian.com/technology/2018/aug/22/us-elections-hacking-voting-machines-def-con.

Howard, Elizabeth, et al. *"Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary."* Brennan Center for Justice, Brennan Center for Justice at NYU Law, 13 Aug. 2019, www.brennancenter.org/our-work/analysis-opinion/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

Jacob, Léo-Paul. *"An Exploration into the Growth of Russian Cyber Warfare."* NAOC, NATO Association of Canada, 25 Mar. 2017, natoassociation.ca/russias-cyber-warfare/.

Kamarck, Elaine and Darrell M. West. *"Dirty Tricks in the Digital Age."* Washington, D.C.: Brookings Institution Press, 2020. doi:10.7864/j.ctvt9k60n.

"Key Findings of the Mueller Report: ACS." American Constitution Society, American Constitution Society for Law and Policy, 24 July 2019, www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.

Khan, Mariam. *"Trump Suggests He'd Oppose USPS Funding to Hurt Mail-in Voting, Then Says He Won't."* ABC News, ABC News Network, 13 Aug. 2020, abcnews.go.com/Politics/trump-opposes-funding-usps-bid-block-vote-mail/story?id=72353322.

Kim, Noah Y. *"Fact-Checking Donald Trump's Tweet Firing Christopher Krebs."* PolitiFact, The Poytner Institute, 18 Nov. 2020, www.politifact.com/factchecks/2020/nov/18/donald-trump/fact-checking-donald-trumps-tweet-firing-christoph/.

Leong, Dymples. *"Securing Elections and Beyond: Lessons for Singapore from Canada's 2019 federal election."* Report. S. Rajaratnam School of International Studies, 16 Nov. 2020. Accessed November 3, 2020. doi:10.2307/resrep24324.7.

Martinez, Gabriela. *"How the U.S. Is Trying to Improve Election Security Ahead of 2020."* PBS, Public Broadcasting Service, 17 June 2019, www.pbs.org/newshour/politics/how-the-u-s-is-trying-to-improve-election-security-ahead-of-2020.

McKenzie, Timothy M. *"Is Cyber Deterrence Possible?"* Air University Press, 14 Nov. 2017. http://www.jstor.org/stable/resrep13817.10.

Mergerian, Chris, and Wilber, Del Quentin. *"Mueller Submits Trump-Russia Investigation Report but Doesn't Recommend Additional Indictments."* Los Angeles Times, Los Angeles Times, 22 Mar. 2019, www.latimes.com/politics/la-na-pol-robert-mueller-russia-investigation-report-filed-20190322-story.html.

Nair, Devi et al. *"Beyond the Ballot: HOW THE KREMLIN WORKS TO UNDERMINE THE U.S. JUSTICE SYSTEM."* Center for Strategic and International Studies (CSIS), 2019. 33-35. doi:10.2307/resrep22556.8.

Panetta, Alexander and Scott, Mark. *"Unlike U.S., Canada Plans Coordinated Attack on Foreign Election Interference."* Politico, 4 Sept. 2019, www.politico.com/story/2019/09/04/canada-foreign-election-meddling-1698209.

Polityuk, Pavel, and Zawadzki, Sabina. *"Ukraine Says Russia Follows Pre-Georgia War Scenario in Crimea."* Edited by Timothy Heritage, Reuters, Thomson Reuters, 28 Feb. 2014, www.reuters.com/article/us-ukraine-crisis-turchinov/ukraine-says-russia-follows-pre-georgia-war-scenario-in-crimea-idUSBREA1R1WN20140228.

Rappeport, Alan, and Nicholas Fandos. *"Mnuchin Defends Plan to Lift Sanctions on Russian Oligarch's Companies."* The New York Times, 10 Jan. 2019, www.nytimes.com/2019/01/10/us/politics/mnuchin-russia-sanctions.html.

Rotondo, Annachiara, and Pierluigi Salvati. *"Fake News, (Dis)information, and the Principle of Nonintervention: Scope, Limits, and Possible Responses to Cyber Election Interference in times of Competition."* The Cyber Defense Review, 2019, 209-24. doi:10.2307/26846129.

Rumer, Eugene. *"The Primakov (Not Gerasimov) Doctrine in Action."* Carnegie Endowment for International Peace, 5 June 2019, carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

"The Republicans' Defensiveness about Russian Hacking Is Revealing." The Economist, The Economist Newspaper, www.economist.com/united-states/2018/07/21/the-republicans-defensiveness-about-russian-hacking-is-revealing.

Swanson, Emily and Tucker, Eric *"Poll: Americans Concerned by Foreign Interference."* AP NEWS, Associated Press, 2 Oct. 2020, apnews.com/article/election-2020-chicago-elections-archive-voting-44e78a1906754ba20d2af0f457ffb902.

Office of the Special Counsel. *"Report On The Investigation Into Russian Interference In The 2016 Presidential Election."* II, U.S. Department of Justice, 2019, pp. 2–182. www.justice.gov/storage/report.pdf.

Villasenor, John. *"Deepfakes, Social Media, and the 2020 Election."* The Brookings Institute, Brookings Press, 3 June 2019, www.brookings.edu/blog/techtank/2019/06/03/deepfakes-social-media-and-the-2020-election/.

Zimonjic, Peter. *"Liberals' Election Reform Bill Becomes Law on Last Day of Parliamentary Sitting."* CBC News, CBC/Radio Canada, 13 Dec. 2018, www.cbc.ca/news/politics/liberals-cote-election-reform-1.4945681.