alliance for securing democracy
G | M | F

October Surprise

Simulating a Foreign Interference Crisis on the Eve of the 2020 Election

Nathan Kohlenberg, Research Assistant
October 14, 2020

Executive Summary

The United States, like many other democracies, faces concerted and sophisticated operations aimed at disrupting, delegitimizing, and in some cases altering the outcomes of its elections. While foreign interference operations are not bound by election cycles, elections constitute a unique window of increased vulnerability.

To better understand how well U.S. institutions have adapted since the 2016 election, the Alliance for Securing Democracy conducted a table-top exercise to assess potential gaps in policies and practices by government, social media platforms, and campaigns. The exercise also considered the options, challenges, and trade-offs that politicians, policymakers, and corporate officers might face in the days leading up to the 2020 election.

The exercise was conducted virtually in July 2020 with a bipartisan group of 14 experts representing senior government, political organizing, and technology industry leaders. The results were clear: information sharing stalled, lines of communication were lacking, and distrust was rampant. Parochial interests and the mitigation of personal and organizational risk often took priority over national interests. Meanwhile, many leaders struggled to gather the information they needed to commit to a course of action. Although a simulation can never capture the complexity of the systems and relationships it aims to approximate, this exercise underscores that there is work to be done to improve resilience in all three sectors analyzed: the U.S. government, professional politics, and the technology sector.

Many shortcomings were immediately apparent to the experts who participated, while others became evident in the after-action analysis. Working with the participants and other experts on election interference, we have summarized in this report a number of lessons learned from the exercise in order to spotlight recent progress and remaining challenges.

Our simulation strongly suggested that current policies and structures are insufficient to facilitate the coopera-

tion between stakeholders that would be necessary to mitigate a sophisticated information operation targeting the election. In particular, our participants concluded that response mechanisms remained troublingly dependent on the personal integrity of decisionmakers in Washington and Silicon Valley, and current government and social media policies are insufficiently precise and unambiguous to provide clear guidance in many situations, especially as relate to privacy and First Amendment concerns. Nevertheless, the particular course of the exercise and approaches taken by the participants also shed light on what can be done to build greater responsiveness into the range of public and private institutions responsible for ensuring the integrity of our elections.

The Vulnerability of Elections

Russia's interference in the 2016 U.S. presidential election brought into sharp focus the threat of foreign interference in democracies. Other actors are learning from Russia's playbook, including China, Iran, and domestic actors who increasingly engage in information operations to spread disinformation, gain leverage, or sow doubt in democratic institutions. The emotionally charged atmosphere leading up to elections, when voters may be more vulnerable to disinformation that plays on their expectations and biases, can increase the impact of weaponized information. At the same time, narratives undermining election integrity can undermine their legitimacy, while also suppressing voter participation. Timing is an additional and unique challenge in the run-up to elections. Most information operations are ultimately exposed, but when weaponized information is deployed in the immediate run-up to an election, politicians, journalists, investigators, and media platforms all face a compressed timeline for responding.

Over the past few years, the U.S. government and social media platforms have taken steps to address vulnerabilities to foreign interference, and campaigns have increased their defenses and attention to these issues. Although these steps have fallen short in many areas, particularly in addressing structural gaps that led to previous information-sharing failures, these actors are all focused on the threat. Important reforms undertaken by the U.S. government since 2016 include:

- Providing top election officials in each state with security clearances, allowing them to view intelligence in order to be better prepared for specific threats, and establishing new protocols to allow federal authorities to share information with them.[1]
- Establishing the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) with a specific mandate to fight cyberthreats to critical infrastructure, including election infrastructure.[2]
- Legislating significant penalties for states and individuals engaged in foreign election interference, including sanctions, asset freezes, and travel bans.[3]
- Establishing specific taskforces within the intelligence community, like the Foreign Interference Task Force within the Federal Bureau of Investigation (FBI), with a mandate to identify planned or ongoing attacks on elections, and programs like the Protected Voices initiative (also within the FBI) to facilitate information sharing with political campaigns, technology companies, and other non-public stakeholders.[4]
- Appropriating new federal money to train election staff on cybersecurity issues and fund the purchase of newer, more secure, more auditable election equipment.[5]
- Creating a new Election Threats Executive role within the Office of the Director of National Intelligence tasked with integrating all of the information about election interference across the entire intelligence community.[6]
- Establishing an Election Security Group to facilitate cooperation between the National Security Agency and U.S. Cyber Command with a mandate to "disrupt, deter, and degrade adversaries' ability to interfere and influence U.S. elections."[7]
- Issuing new guidance to campaigns through the FBI on how to secure their operations against foreign intrusion, and how to report suspected intrusions to their local FBI field office.[8]

Additionally, non-government actors have taken some key steps. These include:

- Campaigns hiring security officers specifically tasked with ensuring operational integrity and instituting best practices with respect to cybersecurity and cyber hygiene.[9]
- Political parties developing working relationships with individual candidates and campaigns aimed at

facilitating bi-directional information sharing about election threats.[10]

- Technology firms participating in information-sharing partnerships with intelligence agencies to form clearer pictures of threats and ongoing operations.[11]
- Social media platforms adopting stricter content moderation policies and enforcing these policies with periodic takedowns of networks of coordinated inauthentic behavior.[12]

Despite these steps, stakeholders in and out of government have warned that elections remain too vulnerable to attack. In the words of J. Michael Daniel, chief executive of the Cyber Threat Alliance and a former White House cybersecurity official, "Unquestionably, we are better off than we were in 2016. But better off does not mean that we are where we need to be."[13]

The Simulation

Purpose and Goals

The Alliance for Securing Democracy set out to design a table-top exercise that would explore how well key U.S. institutions are prepared to respond to a major interference operation in the final month of a presidential contest. In particular, we wanted to see if current policies, norms, and structures were sufficient to facilitate cooperation between a range of stakeholders likely to be engaged or implicated by such an event. Our goal was to use a real-time exercise to evaluate how actors would behave and whether new structures were robust enough to facilitate a concerted response. We also sought to identify critical points of failure that could be leveraged by a dedicated and creative adversary. Although the scenario is distinctly American, we hope the lessons learned are broadly applicable to liberal democracies facing foreign interference.

As investigative tools, table-top exercises are inherently limited: no exercise can come close to capturing the breadth and complexity of real-world events. The artificial environment affects the behavior of the participants, and the relationships between participants are inherently mediated by the choices of the game designers. Nevertheless, by asking individuals with many years of real-world experience to participate, we attempted to minimize these distortions. The goal was to draw lessons about how these and other experts might fare in the face of new foreign interference challenges.

Game Design

The diffuse and variable nature of the election interference threat touches on nearly every aspect of our society and will ultimately require a national effort to overcome. Our exercise focused on three essential institutions: the U.S. government, private sector media platforms, and political campaigns. We recruited participants for three teams, representing the National Security Council (NSC), the senior leadership of Facebook (which served as a proxy for the larger ecosystem of social media firms), and the senior staff for a fictional Democratic presidential campaign. Each player was assigned a specific role on their team (show below) and provided a written briefing that enumerated both their responsibilities and specific pieces of intelligence or information about the crisis.

Simulation Teams and Individual Roles		
United States Government	**Facebook**	**Davis Campaign**
National Security Advisor	Chief Operations Officer	Campaign Manager
Secretary of State	Director of Government Relations	Policy Director
Secretary of Homeland Security	Head of Trust and Safety	Chief Counsel
Director of National Intelligence	Chief Technology Officer	Communications Director
Director of the FBI	Chief Security Officer	

In order to make the behavior of the teams as realistic as possible, we sought the participation of individuals who have served in or adjacent to the roles that they were asked to play. The government team included a former

cabinet secretary, a former career ambassador, and several senior veterans of the NSC and intelligence community, with a roughly equal number having served in Democratic and Republican administrations. The Facebook team included experts on information operations and individuals with years of experience in Silicon Valley. The campaign team comprised former senior campaign advisors to presidential candidates of both parties, including an expert in campaign finance law. In order to ensure that participants were not constrained by any real-world professional or reputational considerations, we conducted the exercise under the Chatham House Rule.

The exercise was divided into five parts:

1. An opening briefing on the simulation and the details of the fictional crisis;
2. Breakout sessions for each of the three teams;
3. An update briefing based on the decisions arising from the first set of meetings;
4. Additional breakout sessions in which the teams evaluated and altered their strategy based on new information; and
5. A debriefing and lessons-learned discussion.

This structure encouraged players to reckon with the consequences of their choices in an iterated way, while still being self-contained enough to be conducted virtually in three hours.

Scenario Synopsis

The scenario began 15 days before the 2020 presidential election. It assumed a fictional incumbent Republican president (President Robertson) and Democratic challenger (Senator Davis). Players learned that a video of unknown origin had begun to circulate on social media. This video appeared to show a senior advisor to President Robertson in a private meeting with Saudi Crown Prince Mohammed bin Salman. In the meeting, the advisor appeared to ask the crown prince to cut oil exports, explaining that this would benefit the president's reelection chances, and that in return Saudi Arabia would be permitted to purchase F-35 fighter aircraft from the United States. They also learned that the video was first sent to the campaign of the Democratic challenger, which reported it to the FBI. A fringe American news website posted it to Facebook the following day. The president immediately condemned the video as a forgery and encouraged his intelligence chief to declare it a hoax.

Each player was provided further information specific to their character, which they could choose to share with other players on their team or other teams. All three teams were bedeviled by several fundamental uncertainties:

- Is the video authentic, deceptively edited, substantially manipulated, or fabricated?
- Who recorded the video? Who distributed the video?
- What did the distributors hope to achieve by releasing it two weeks before the election?

The teams were given broad latitude to formulate their responses, and to coordinate and share information with other teams. Each also faced a number of specific decisions, including what information about the video and its origins to release to the public, and what avenues of investigation to prioritize. Based on those decisions, players were given new information, some of which was specific to each team. The government team learned that the FBI had found the tape to be fundamentally unaltered, and that the intelligence community assessed with a high degree of confidence that it had been leaked by the Iranian Revolutionary Guard Corps (IRGC) for the purpose of hurting the president's reelection chances. They also learned that suspicious documents circulating online were forgeries aimed at maximizing the impact of the video. The teams then convened again (simulated as a week after the first meeting and six days before the election) to discuss the new information and adjust their investigative, information-sharing, and crisis-management strategies. During the second meeting, the Facebook leadership team became aware via a press leak that the video was likely authentic and part of an Iran-linked operation.

Lessons

Lesson #1 – Knowledge Is Power (And Power Is Not Easily Shared)

One of the most quickly apparent lessons was that, despite a strong desire to mount a coordinated response, the parties were hamstrung by information sharing constraints. These barriers to information sharing can be broadly categorized as political, legal, and reputational.

Presidential Prerogative

A substantial and immediate obstacle to information sharing came from President Robertson, who viewed the video as an assault on the integrity of his administration. He urged his NSC to characterize the video as a forgery, even when too little evidence had been unearthed to determine its authenticity. The video turned out to be fundamentally authentic, and the president's denials served ultimately to further the worldview that the perpetrators had hoped to advance: democratic leaders are corrupt and dishonest. The government team ultimately overcame the president's pressure once evidence of malign activity became irrefutable during the second round, but this might not be the case in all instances. NSC members were ultimately undeterred by the president's denials, so they wisely did not at any point publicly endorse them, avoiding harm to the national security and federal law enforcement communities.

Once the government team had gathered enough evidence to determine conclusively that the president was acting in bad faith, they prepared to release what they knew, including that the video was authentic, to the press and public. Though this in essence served to validate stolen and weaponized information, the government team reasoned that the cat was out of the bag, and that only transparency could prevent further harm to the credibility of the U.S. government in general and the intelligence community in particular. This episode served as an important reminder that the response mechanisms implemented since 2016 to combat election interference remain potentially beholden to the personal integrity of the individuals in leadership positions. Government officials can be manipulated into participating in or exacerbating foreign interference operations. All participants played political appointees, but were ultimately willing to sacrifice their jobs to protect the integrity of the election. Relying on such integrity in the real world, however, presents an obvious vulnerability that autocrats bent on interference could exploit.

The Privacy Problem

During this exercise, the Facebook senior leadership team saw activity on their network amplifying the leaked video but could not determine if the activity was coordinated and inauthentic. This uncertainty complicated information sharing with both the public and the FBI, because Facebook sought to balance the rights to privacy and expression of their users with the public interest of unmasking those involved in a coordinated informational attack on the election. The perpetual challenge of establishing territoriality further complicated the question. The video had been shared to Facebook by an American news website, albeit one with a spotty reputation, and Facebook made protecting the right of American voters to engage with the press a high priority. Accounts outside the United States could be held to a somewhat different standard, but many other jurisdictions in which Facebook operates offer their own privacy protections, like the Global Data Protection Regulation in the European Union. Because of the global nature of the social media ecosystem, laws on other continents can have major implications for what data social media companies share with law enforcement.

Information sharing between public and private groups remains problematic. This is a delicate issue, because authoritarian states seek to normalize the abrogation of privacy rights, especially online. Any solution that allows greater information sharing from Silicon Valley to Washington must ensure the continued protection of users' privacy and personal data integrity. Anonymization tools that strip away personally identifiable information

prior to sharing data offer one promising way forward. Better established modes of information sharing that protect user privacy would also allow social media companies to share more data with campaigns, which should be encouraged in the case of high-profile interference in elections.

Due Diligence

The campaign team possessed the least information in this exercise, and as a result had the least power. Faced with a decision over whether to conduct an exhaustive or minimal investigation to determine if their own staff had told the press about the video, the team reached a split decision. A thorough investigation could have raised the prospect of confirming that the campaign participated in the proliferation of disinformation, which would increase their liability and violate an election integrity pledge that their candidate had made, thereby muddling her message at the worst possible time. Simply put, campaigns do not have the resources, expertise, or unbiased perspective necessary to investigate information operations or election interference attempts. Prior good-faith working relationships with law enforcement and social media platforms could help facilitate the flow of information between all parties, provided that the campaign point of contact is insulated from the partisan atmosphere of the campaign at large.

Lesson #2 – Timing Matters

A clear and consistent theme that emerged from the exercise was that both the effects of and appropriate responses to election interference are timing dependent. Appropriate courses of action for responding to an information operation occurring far from an election, like fact-checking by traditional media or contextualization by key validators, can be ineffective or even counterproductive in the compressed timeframe immediately preceding an election. This window of vulnerability is more complex due to early voting and mail-in voting, particularly around the 2020 election. By November 3rd a substantial share of votes will have already been cast, rendering new information or counternarratives only partially effective.

Publicize or Prosecute

Many information operations involve international criminal activity. This is especially true of "hack and leaks," which typically rely on the theft or illegal recording of politically embarrassing activities or statements. In such cases, senior law enforcement officials are likely to face institutional pressure to preserve evidence and intelligence, as well as sources and methods, that might be central to future prosecutions. Democracies are right to place a premium on preserving the possibility of bringing bad actors to justice in a court of law. Nevertheless, this impulse can be taken advantage of by those aiming to do immediate harm to an upcoming election.

In this exercise, the FBI acquired substantial evidence that Iranian Revolutionary Guard Corps commanders had organized and executed this information operation and violated U.S. law in the process. But given that the individuals responsible would be nearly impossible to bring into U.S. custody, the FBI Director ultimately authorized the release of information to the public, revealing the perpetrators of the conspiracy. Preserving evidence for a future trial that was unlikely to occur was deemed less important than giving voters the opportunity to contextualize new information introduced immediately prior to an election. There is no one-size-fits-all rule that can determine when it is appropriate to reveal details of an investigation in order to minimize the impact of an ongoing attack. Key considerations should include the magnitude of the attack, the realistic prospects of the perpetrators facing prosecution, and the ameliorative impact that disclosure could have. These guidelines should be applied equally regardless of whether the attack targets the incumbent or the challenger.

Content Immoderation

The Facebook senior leadership team worked hard to enforce the company's established guidelines for managing content of ambiguous veracity and unknown origin. Technical investigations into the video were initially

inconclusive, so with no clear evidence that it was illegally acquired, Facebook allowed the video to continue to circulate for days. This was consistent with a neutral application of Facebook's guidelines, but some on the team questioned whether this static set of guidelines was too inflexible and easy for a dedicated adversary to manipulate. Some players proposed that social media companies should consider adopting more restrictive content guidelines for campaign or voting-related weaponized content during the weeks immediately preceding major elections. In September 2020, two months after our exercise, Facebook took a major step in this direction by banning new political ads in the week prior to the election in order to prevent the introduction of new, potentially manipulated narratives during the window in which it would be too late for proper fact-checking and reporting. Facebook also promised to label premature declarations of victory by candidates and parties, and link to official results. Twitter quickly followed suit with stricter rules on posts promoting false information about voting or voter fraud, and also promised to remove posts that prematurely or inaccurately claim victory.

These are positive steps that will improve resilience against particular forms of weaponized information. Unfortunately, no content moderation policy will completely insulate corporate officers from having to make difficult, situationally-specific judgment calls about what enforcement actions best uphold their values and the public interest. Weaponized information is a challenge throughout the political cycle, not just when elections are imminent. Nevertheless, given that the preservation of election integrity is an explicit priority for these firms, and that the impact of weaponized or manipulated information is fundamentally different when there is no time for it to be contextualized, social media platforms should ensure that administrators have the capacity and mandate to enforce policies in a forward-leaning manner ahead of major elections.

Lesson #3 – Location, Location, Location

The territoriality of the actors involved in the disinformation operation complicated the decision making of all three teams. Without knowing the location or context of the video's production, neither the government nor Facebook team could confidently assert what laws or policies applied. For the government, the ambiguity of whether the actors responsible were foreign or domestic made it difficult to know immediately what standard of scrutiny and which legal and policy frameworks should be applied. For the Facebook team, the question of whether the video was altered or authentic complicated the same question. And while social media companies' new labeling policies for government-affiliated media is an important step, foreign election interference is frequently laundered through domestic institutions and businesses.

Policy Precision

The government team struggled to categorize the nature of the attack, even after the broad fact pattern had become clear. By leaking unaltered evidence of attempted solicitation of Saudi assistance by members of the president's staff, the IRGC had deployed stolen and weaponized information, but the video itself did not constitute disinformation. Further complicating their decision-making, the chain of custody of the video was unclear, but passed unambiguously through the hands of U.S. media. Effective policy must have clear and consistent definitions and thresholds with respect to what constitutes foreign election interference, disinformation, election tampering, voter suppression, and other events that might necessitate a law enforcement response.

The Facebook team struggled with the same chain of custody and territoriality questions but had even less information. Initially unsure of the video's veracity, they left it on their platform with a disclaimer. Once its origins were revealed by a press leak, the team found itself in sharp disagreement over whether its weaponization or its authenticity was the salient issue, ultimately voting 3-2 to take it down. Current Facebook policies prohibit hacked or stolen materials "except in limited cases of newsworthiness." But by definition, major interference operations will be newsworthy, and will be reported on by American news outlets, limiting the impact of this prohibition. Facebook's current policies define "voter interference" very narrowly, and tie it to voter suppression efforts, like providing false information about how and when to vote, or efforts to misrepresent the outcome

of recent contests. Social media companies face a torrent of weaponized information, some foreign, but much domestic. Policies must balance the right to expression with the responsibility to prevent voter suppression and disinformation.

Lesson #4 – Keep Your Friends Close

An unanticipated development came late in the simulation as the government sought to coordinate a collective response with European allies. A former ambassador serving as the fictional Secretary of State pointed out that the nature of the administration's conduct would make cooperation with allies impossible. By exposing genuinely underhanded behavior on the part of the administration, Iran had dealt a blow to the very transatlantic cohesion that would be necessary to impose costs on Iran. This dynamic underscores the vulnerability of our alliances to weaponized information. In the past, we have seen information warfare techniques honed in one nation or election, and then deployed in another. Alliances between liberal democracies are not only a key asset to be leveraged in resisting authoritarian interference, they are also a target of such operations themselves. In the past, authoritarian regimes like Russia and Iran have sought to widen and exacerbate divides between allies, especially the United States and Europe, and have used weaponized information to do so.

Democracies find themselves locked in a competition of systems, and authoritarian states aim to peel away members of the coalition using interference and narrative manipulation to divide liberal states. Given that we all face many of the same threats from the same actors, learning from the experiences of other democracies can provide insights, particularly for smaller countries, that will help resist these attacks. This cooperative approach has the added benefit of strengthening alliance relationships and making them more resilient in the face of interference.

Conclusion

Election interference through weaponized and manipulated information will remain a pernicious problem for all democracies for the foreseeable future. As with other systemic challenges introduced by new communication technologies, it can be managed in ways consistent with the preservation of both free expression and privacy that distinguishes liberal regimes from authoritarian ones. Major steps have been taken over the last four years to improve the ways in which American institutions respond to this challenge. For example, technology firms are more vigilant in the face of election interference and the intelligence community has new disclosure requirements. Yet, our exercise found that existing laws and policies are insufficient to provide decision-makers the guidance to prevent election interference in real time. Too often, relationships remain insufficient to allow the level of information sharing necessary to coordinate responses among key stakeholders.

On the government side, decision-makers may not be sufficiently insulated from the political consequences of responding to a foreign attack that is aimed at benefiting one candidate over another. Institutional biases towards keeping information private, especially if it could be evidence in a future investigation, also remain a persistent obstacle to critical information sharing. Among Silicon Valley firms, new guidance on how to manage potentially weaponized content remain compromised by loopholes like "newsworthiness" that encourage corporate leaders to punt on difficult questions. Meanwhile, formal information sharing remains under-institutionalized and mired in jurisdictional privacy challenges. Finally, political campaigns are more aware of the threat today than four years ago, but they remain beholden to the logic of electoral politics, a dynamic reinforced by our exercise.

Building resilience will require changes in how we spread, evaluate, and process the firehose of information we all face today. Although this exercise focused on the challenges faced by the United States, many of the problems have analogues in European, Asian, African, and other democracies. Just as authoritarian states learn each other's tools and techniques for suppressing dissent and engaging in disinformation outside their borders, liberal democracies need to establish new norms surrounding election protection, information sharing, and internet governance. Table-top exercises of this sort offer one way to experience new threats and evaluate new approaches. This exercise explored just one of many possible threats, so additional efforts are warranted to develop effective real-world responses. These should focus on establishing open, candid lines of communication that give leaders in government, technology, and politics the tools and guidelines they need to make sound decisions that protect and strengthen democratic institutions and processes.

Endnotes

1 "Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges before the 2020 Elections," Government Accountability Office, February 2020.
2 Cynthia Brumfield, "What is the CISA? How the new federal agency protects critical infrastructure from cyber threats," Christian Science Monitor, July 1, 2019.
3 "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," White House, September 12, 2018.
4 Adam S. Hickey, "Statement of Adam S. Hickey, Deputy Assistant Attorney General, Justice Department, Before the Subcommittee on National Security, Committee on Oversight and Reform, U.S. House of Representatives, at a hearing entitled 'Securing U.S. Election Infrastructure and Protecting Political Discourse,'" U.S. House of Representatives, May 22, 2019.
5 Christina A. Cassidy, "More election security funds headed to states as 2020 looms," Associated Press, December 19, 2019.
6 "Director of National Intelligence Daniel R. Coats Establishes Intelligence Community Election Threats Executive," Press Release, Office of the Director of National Intelligence, July 19, 2019.
7 "U.S. Cyber Command, NSA Poised to Support U.S. Election Security," National Security Agency Central Security Service, January 29, 2020.
8 "FBI Boston Division Issues Public Guidance on 2020 Election Security," Federal Bureau of Investigation, Boston Office, September 28, 2020.
9 Uri Friedman, "'No One Is Accountable for This': Why the 2020 Campaigns Are Struggling With Security," The Atlantic, September 5, 2019.
10 Colleen Long and Christina A. Cassidy, "2020 campaign staffers being trained to handle cyber threats," Associated Press, May 3, 2019.
11 Christopher Wray, "Tackling the Cyber Threat Through Partnerships and Innovation," Remarks to the Boston Conference on Cybersecurity, Boston College, March 4, 2020.
12 Hannah Murphy, "Twitter toughens up policy on misleading election posts," Financial Times, September 10, 2020.
13 Robert McMillan, "Election Officials Are Vulnerable to Email Attacks, Report Shows," Wall Street Journal, July 26, 2020.