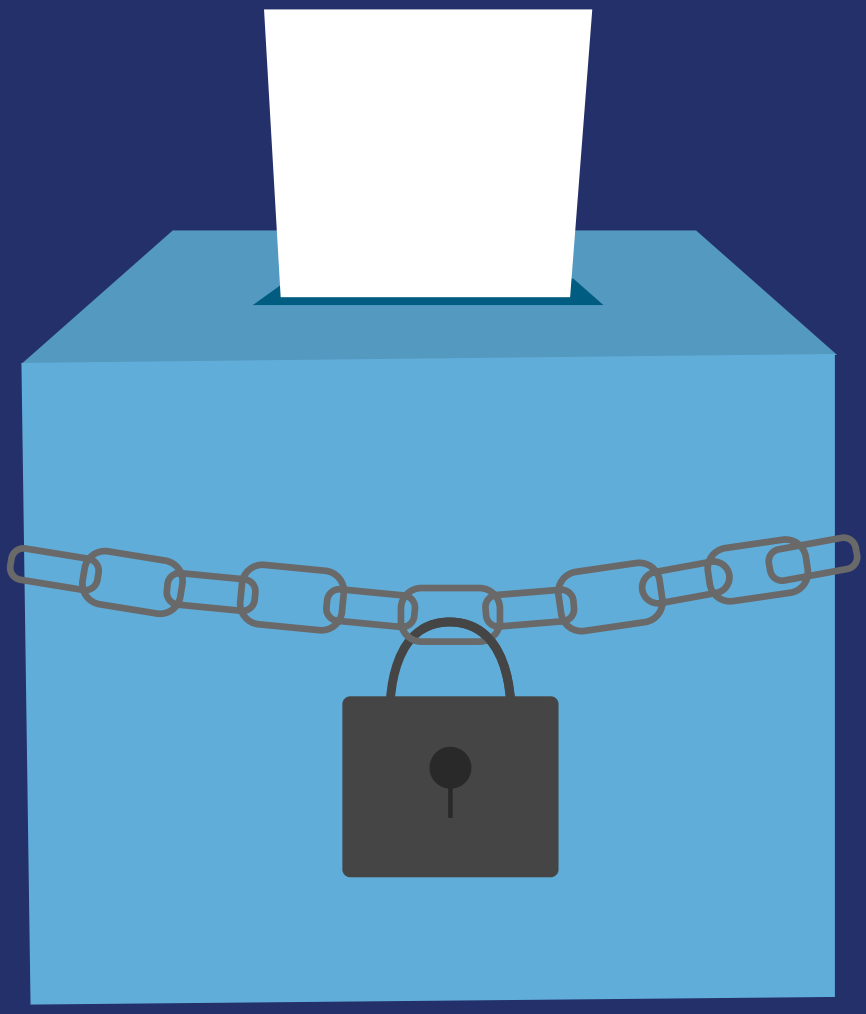
US Elections Disinformation Tabletop Exercise Package



US ELECTIONS DISINFORMATION TABLETOP EXERCISE PACKAGE

OCTOBER 2020

OUMOU LY
JORHENA THOMAS

ASSEMBLY:
DISINFORMATION

A JOINT PUBLICATION FROM:

ASSEMBLY:
DISINFORMATION

BERKMAN
KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

SCHOOL *of*
INTERNATIONAL
SERVICE

Online foreign interference, coordinated influence operations, and disinformation have become the new normal for elections and other democratic processes. These pernicious problems pose threats to the 2020 US General Election; and, we should expect them to persist in future US elections as well as others held around the world for years to come.

Countering these issues requires an unprecedented effort among a diverse group of stakeholders – ranging from the US national security community to state/local election officials to Internet platforms and journalists. They must be able to anticipate and react to a wide range of political and cybersecurity challenges expected to arise in the November 2020 election.

This publication was inspired by conversations between the co-authors and by discussions in the Assembly Forum, which is a part of the Berkman Klein Center's Assembly: Disinformation Program. The Assembly: Disinformation Program convenes participants from academia, industry, government, and civil society from a broad variety of disciplinary perspectives to explore disinformation in the public sphere.

SUGGESTED CITATIONS

APA

Ly, O., & Thomas, J. (2020). *US elections disinformation table exercise package. Assembly: Disinformation*, Berkman Klein Center for Internet & Society. https://cyber.harvard.edu/publication/2020/US-elections-disinformation-table-top-exercise-package

Chicago (Bibliography)

Ly, Oumou and Jorhena Thomas. "US Elections Disinformation Table Exercise Package," Assembly: Disinformation, Berkman Klein Center for Internet & Society (2020), accessed on [Month Day, Year], https://cyber.harvard.edu/publication/2020/US-elections-disinformation-table-top-exercise-package

Chicago (Footnote)

Ly, Oumou and Thomas, Jorhena, "US Elections Disinformation Table Exercise Package," Assembly: Disinformation, Berkman Klein Center for Internet & Society (2020), accessed on [Month Day, Year], https://cyber.harvard.edu/publication/2020/US-elections-disinformation-table-top-exercise-package.

MLA

Ly, Oumou and Thomas, Jorhena. "US Elections Disinformation Table Exercise Package." Assembly: Disinformation, Berkman Klein Center for Internet & Society, 2020. Web. [Day Mon. Year]. <https://cyber.harvard.edu/publication/2020/US-elections-disinformation-table-top-exercise-package>.

Bluebook

Oumou Ly and Jorhena Thomas. US Elections Disinformation Table Exercise Package (2020), *available at* https://cyber.harvard.edu/publication/2020/US-elections-disinformation-table-top-exercise-package

TABLE OF CONTENTS

AUTHORS' NOTE

AS THE WORLD CONTENDS with the COVID-19 pandemic, Americans are navigating an eruption of racial tensions and protests resulting from long standing structural racism. Sustained attention on these high interest topics has proven them ripe for disinformation, conspiracy, and information operations, including by foreign states, designed to degrade public confidence in American democratic processes. Influence operations also work to sow chaos and induce perceptions of a devolving society.

Academics, government officials, and other experts have postulated that state actors propagating disinformation do so largely by exploiting preexisting tensions, and that they amplify discord rather than manufacturing it. In many ways, the sociopolitical fissures and fractious debates that made the United States vulnerable to information warfare by adversarial nation states during the 2016 elections are more significant today. Accordingly, the opportunities for exploitation are more numerous. Ongoing protest activity provides adversaries the opportunity to inject inflammatory false narratives; lack of a national plan to mitigate the spread of COVID-19, coupled with political attack on traditionally authoritative sources of public health information provide threat actors fodder to sow confusion; and partisanship continues to be an avenue for exploitation for adversaries.

In addition to disinformation, this election will have other vectors for exploitation. The use of electronic voting machines in many election jurisdictions across the country, including those with demonstrated security vulnerabilities, is of significant concern, along with vulnerabilities in voter registration databases. In addition, the widespread use of absentee voting due to the COVID-19 pandemic could affect public perception of the integrity of the election. As what is sure to be a contentious election approaches, it is important to view the election within the context of these challenges.

We felt compelled to create a resource that our colleagues across government and industry could use to prepare for the election. This document identifies four key stakeholder groups: state and local election officials, technology platforms, professional media organizations, and the United States Intelligence Community (USIC). As the considerations that drive decisions on interventions vary by audience, this document contains four exercises, with one exercise tailored to the particular considerations of each group. Although each exercise is tailored to challenge a specific stakeholder group, each exercise also features questions for other stakeholder groups to encourage a broad dialogue about responses.

Exercises in this document feature a number of cross-cutting themes, which we think of as the constituent parts of an election: Namely, (1) electoral systems, processes, and infrastructure, which state and local officials will be interested in; (2) public perceptions of the electoral system as a whole, which media organizations, the USIC, and technology platforms are concerned with; and (3) the peaceful transition of power, which is a hallmark of democracy and critical for all audiences.

Protecting our elections in this groundbreaking time requires innovation, assumption of a transparent posture with regard to the limitations of our current frameworks, and close interdisciplinary and cross-sectoral collaboration. Tabletop exercises in this document are meant to encourage key actors to assess their plans and think about how to strengthen them, using realistic scenarios to drive discussion. We hope that, through discussion, participants will benefit from learning how their counterparts and colleagues from other sectors might approach responding to the same defined incident.

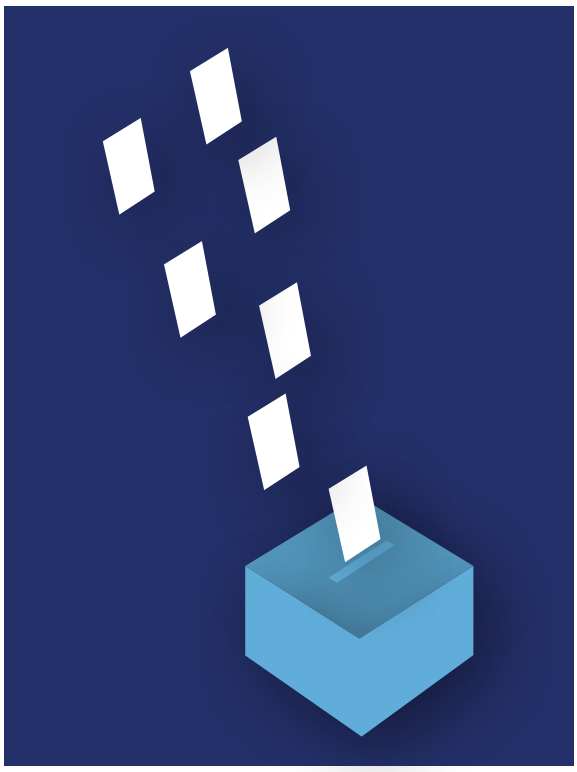
Moreover, the exercises in this document aim to illustrate that developing a sufficiently robust framework for combating election-related, COVID-19 related, or racialized disinformation must be a top national security priority. It is our hope that these exercises encourage greater coordination among the named stakeholder groups, assist in the development of new contingencies, and contribute to our growing collective understanding of the impact of disinformation across the body politic.

Oumou Ly
Berkman Klein Center for Internet and Society at Harvard University

Jorhena Thomas
American University School of International Service

INTRODUCTION

THE CHALLENGE of mitigating and responding to disinformation has taken on a new importance since the 2016 election, even as a precise measure of its impact remains methodologically elusive. Academics and practitioners alike have produced a large body of research and writing on this topic and have contributed much to the study of disinformation, as well as how to combat it. One area that warrants additional attention in the disinformation space is that of structured exercises to test the efficacy of myriad plans, procedures, and policies related to disinformation response across sectors.



The purpose of this document is to attempt to fill this gap. This document provides a set of realistic disinformation-focused scenarios and discussion questions. Content in this document was crafted with the aim of advancing efforts to address, counter, defend the public against, and ultimately, mitigate the impact of disinformation on public discourse in relation to a key democratic foundation: elections.

In light of the unique confluence of challenges we expect will influence the November 2020 election, in addition to ongoing influence efforts by both foreign and domestic malevolent actors, this set of TTX scenarios is meant to encourage key actors to assess their plans and think about how to strengthen them, using realistic scenario fact patterns to drive discussion.

About this Document: This document uses the tabletop exercise (TTX) approach. TTXs can be used to enhance general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the prevention of, mitigation of, response to, protection from, and recovery from a defined incident. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions.

Who This Document is for: This document identifies four key actor groups that have a stake in the disinformation problem in the United States, in addition to having a significant role in addressing it. These are: state and local election officials, technology platforms, professional media organizations, and the United States Intelligence Community. However, the scenarios and discussion questions are useful for a range of individuals and organizations who want to better understand the challenges and limitations faced across the public and private sectors, including universities.

How to Use This Document: These exercises are designed primarily as a basis for structured internal or interagency/interorganizational TTXs. Readers who independently wish to use the scenarios as a part of a structured TTX might find it helpful to read "Appendix A: Conducting a Structured TTX."

This document is divided into four sections. Each section includes one exercise that can be run independently of the others.

Each scenario begins with background information summarizing the considerations for deploying interventions against disinformation. This background is followed by contextual notes for each scenario, including: the particular election implicated, whether a close race for the US Senate, or a US Presidential race; and any information particularly relevant to the hypothetical.

Although exercises are tailored to the challenges unique to particular audiences, each scenario contains challenges pertinent to each audience and can be used for any of the four audiences targeted in this document. Similarly, each scenario is followed by a set of discussion questions tailored to the relevant audiences.

SCENARIO OVERVIEW

SCENARIO	DESCRIPTION	KEY OBJECTIVES
Election Night Foreign Influence Operation **Primary Audience:** State and Local Election Officials	A cyberattack on voting machines in select counties causes frustration and distrust among voters. It is used as a basis for the spread of sensationalized claims that cast doubt on the impartiality of state officials.	1) Examine current plans and procedures 2) Explore cascading effects of an event that leads to the spread of false information 3) Identify crucial action points that can help to anticipate and avoid opportunities for disinformation to develop
Disrupted Voter Registration Drive **Primary Target Audience:** Technology Platforms	One month before the election, a coalition of civil rights organizations organizes a virtual voter registration drive on social media platforms. The event is inexplicably disrupted, and a brigade of accounts engage in a coordinated effort to scapegoat platforms and government officials for the disruption.	1) Evaluate current procedures and best practices, and consider adaptations needed 2) Consider investments in fact-checking resources or other measures to enhance public perceptions of reliability and accuracy of content 3) Test assumptions about users' ability to identify false content 4) Identify gaps in content management efforts
Hack and Leak **Primary Audience:** Professional Media Organizations	A major print exclusive indicates that the email server of the election commission in a swing state has been infiltrated by an unknown actor. These events call into question the state's ability to conduct the electoral process with full integrity on November 3.	1) Evaluate current journalistic best practices and consider adaptations needed 2) Discuss measures to enhance public perceptions of balance, objectivity, and accuracy, especially in relation to elections 3) Identify areas of greatest concern for readers/viewers, and consider shifting resources accordingly

Vote Tally Discrepancies: United States Intelligence Community **Primary Audience:** United States Intelligence Community	The election is disrupted by reports of a cyber intrusion by a foreign adversary. As a coordinated information operation related to the intrusion complicates an already tense situation, the USIC must determine whether and to what extent it will make its findings about the intrusion public.	1) Evaluate current plans and procedures 2) Explore feasibility of the development of interagency guidelines to drive actions related to disinformation 3) Consider development of common definitions for key terms in the disinformation arena 4) Identify areas of agreement and of diversion, and evaluate their implications

EXERCISE 1: ELECTION NIGHT FOREIGN INFLUENCE OPERATION (STATE AND LOCAL ELECTION OFFICIALS)

EXERCISE 1: ELECTION NIGHT FOREIGN INFLUENCE OPERATION

(STATE AND LOCAL ELECTION OFFICIALS)

THE SECURITY OF OUR electronic voting systems and public confidence in our electoral processes are of chief importance to state and local election officials. In addition to maintaining the integrity of election-related hardware and software, election officials play a particularly important role in keeping voters informed with accurate, updated information about the timing, locations, and methods for casting ballots.

Communications from election officials are key targets of attack. Malevolent actors looking to disrupt our elections use disinformation to discourage, mislead, intimidate, or confuse segments of the population with the aim of minimizing the electoral impact of certain groups. These tactics include, but are not limited to: sensationalizing information that is essentially accurate, distorting information, and creating new false claims. For this reason, it is crucial that election officials are prepared to defend against the range of disinformation techniques likely to influence their work.

In the scenario that follows, as voting proceeds, the election is disrupted by reports of a cyber intrusion by a foreign adversary. As a result of the intrusion, voting precincts with large percentages of minority voters cannot certify their votes or must examine a path forward for conducting the election again.

Contextual Note: In a state viewed by both political parties as a critical "swing state," the outcome of the US Senate race will determine which party will assume majority status in the US Senate at the commencement of the next Congress. In the counties implicated in this scenario, voting is conducting by a direct-recording electronic (DRE) voting system[1] equipped with a voter-verified paper audit trail (VVPAT).[2] Other counties in the state rely on other forms of voting, including hand-marked paper ballots.

- *Inject 1:* Citing concerns about the spread of the novel coronavirus at indoor polling locations, state officials announce a reduction in polling locations in the state's three most populous counties in the months proximate to the election: County R, County S, and County T. These counties contain the state's largest distributions of African American and Latino-American voters, and the decision is decried by voting rights organizations and the public at large as a deliberate act of voter suppression.

- *Inject 2:* In response to this criticism, the state's Secretary of State announces via public statement that polling location closures reflect an attempt to control the spread of infectious disease rather than an attempt at suppressing the vote of a particular demographic, and that any registered voter could cast a ballot by mail.

1 An electronic voting system which and tallies votes directly. DREs are used in nearly half of all US states. See https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx; https://www.verifiedvoting.org/verifier/#

2 A VVPAT allows the voter to verify their vote selection before it is tabulated by the DRE system. See https://www.nist.gov/system/files/documents/itl/vote/jlh-vvpat-design-transparency.pdf

- *Inject 3:* As voting proceeds on the day of the election, long wait times at polling locations in Counties R, S, and T prompt frustration among voters, who document their concerns on social media. This activity aggregates into a trending topic on social media platforms as professional broadcast organizations arrive at polling locations to air the voting process in real time.

- *Inject 4:* A small percentage of voters attempting to cast a "straight ticket" ballot in Counties R, S, and T report to poll workers that voting machines have printed their vote selections incorrectly. Upon interrogation of these claims, IT staff in County R indicate to poll workers that machines printing vote selections incorrectly were infected with malicious software which "flips" votes.[3] Once county election officials are alerted, state election officials issue a notice directing any machines printing ballots incorrectly to be powered off.

- *Inject 5:* As malware-infected voting machines are powered off, voting wait times increase quickly and exponentially. Television crews record voters approaching polling stations in Counties R, S, and T, inquiring about the cause of long wait times, and quickly leaving once voters standing in line provide wait time information. This reporting causes a significant uptick in online discussion about the state's voting process, in addition to increased mainstream media coverage of the event.

- *Inject 6:* As voting continues, the Secretary of State holds a press conference indicating that a "small percentage" of voters were impacted by the attack, that they were able to successfully cast provisional ballots in lieu of voting via corrupted machines, and that as no further intrusion could be accomplished, the electoral process would proceed with full integrity. In response to a question from a reporter about whether all voters who voted on a corrupted machine were able to cast provisional ballots, the Secretary of State indicates that not all voters impacted by the attack alerted poll workers about changes to the ballot. This leaves the public to infer that it is likely some voters inadvertently cast ballots of candidates they did not intend to vote for due to machine-error.

- *Inject 7:* After this press conference, a large number of seemingly inauthentic social media accounts begin commenting on the Secretary of State's press conference, claiming that it is likely that tens of thousands of voters used corrupted machines unknowingly. These accounts also point out (accurately) that the state cannot correct ballots cast incorrectly due to machine failure. Moreover, they accuse officials of a racist cover-up and attempt to suppress the minority vote.

- *Inject 8:* As the election continues into the evening, voters begin to leave before casting ballots due to extraordinarily long wait times. Mainstream publications decry the state's voting process as a historic failure, and an act of racism.

- *Inject 9:* When the polls close, election officials announce that they will examine the results of the election and determine whether they can certify the result, given the documented cyber intrusions and immense public interest in the election.

3 Computer scientists have simulated infiltration of DREs with malware programmed to alter vote selections. In jurisdictions which use DREs without a VVPAT, voters cannot verify their vote selections before casting their ballots and are thereby unable to alert poll workers to machine error or failure. See, e.g., https://citp.princeton.edu/our-work/votingsummary/; https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf.

DISCUSSION QUESTIONS: STATE AND LOCAL ELECTION OFFICIALS

1. How might state and local election officials work to ensure they are prioritized as the most current and authoritative sources of information as these developments unfold, and in their aftermath?

   2a. How much information about the cause of the disruption, if any, would county officials publicize?

   2b. How would state officials publicize information on matters for which there are varying or limited degrees of certainty?

3. In the event of a disruption like the one outlined in this scenario, would polling locations be prepared to administer voting by other methods? For instance, are provisional ballots, hand-marked paper ballots, optical scan machines, or other methods immediately available in sufficient supply on Election Day?

4. How would your state's county election office manage the public relations fallout from the perception that it engaged willfully in voter suppression?

5. How would officials work to explain the disproportionate racial impact of this intrusion?

6. In a scenario like this, it is unlikely that the voting machine vendor could provide an estimation of the number of votes "flipped," much less determine the voter's original intent. How might state officials work to assuage public concern about the extent to which the election was impacted by the intrusion?

7. What measures might you take to address online narratives noted in Inject 7 of the scenario?

8. Does your organization already have policies and procedures in place for managing disinformation that arises before, during, or after an election?

DISCUSSION QUESTIONS: UNITED STATES INTELLIGENCE COMMUNITY

1. If your agency became aware of the cyberattack as voting proceeded, how would it go about alerting state and/or local election officials? At what confidence level do you reveal an attack is in progress? Which officials would be prioritized for the initial disclosure?

2. What immediate steps would your agency require or ask of election officials or voting machine vendors? By what means would those requests be communicated? What legal authority does the USIC have to intercede and at what level?

3a. Based on the scenario above, is your agency likely to advise state officials to publicize the cause of the disruption? Why or why not?

3b. Which details of the intrusion would be authorized for release to the public? Which details would be strictly need-to-know?

3c. At what confidence level do you reveal possible sources of the attack?

4. What resources or assistance might your agency offer to officials to mitigate the impact of the intrusion?

DISCUSSION QUESTIONS: PROFESSIONAL MEDIA ORGANIZATIONS

1. How would your organization frame the day's events? In addition to informing the public about these important election related developments, what specific objectives would guide your coverage decisions?
2. Given the opportunity to choose, would you elect to prebunk or debunk the false narrative that emerges in the hours after the intrusion? What considerations would inform your decision?
3. Which experts might your organization choose to amplify to provide accurate information about the election?

DISCUSSION QUESTIONS: TECHNOLOGY PLATFORMS

1. How would your company work to ensure that the authoritative sources of information on these developments are prioritized above less-credible sources in real time? What criteria would your company use to identify authoritative sources?
2. In the event that accounts engaging with or amplifying false narratives cannot be attributed, appear authentic, or are not directly violating terms of service, would your company work to curtail the reach of false content related to the election? If so, how? If not, why?
3. Would your company attempt to disclose to users, either on an individual basis or as a public notice, that they engaged with false content related to the election?

EXERCISE 2: DISRUPTED VOTER REGISTRATION DRIVE (TECHNOLOGY PLATFORMS)

EXERCISE 2: DISRUPTED VOTER REGISTRATION DRIVE

(TECHNOLOGY PLATFORMS)

INTERNET INTERMEDIARIES and online platforms are at the forefront of the discussion on disinformation. In the United States alone, social media platforms are used by millions of organizations and individuals daily to share news and opinions, to connect with others, and to disseminate messages to large audiences. Social media platforms were originally developed to make communication easier, cheaper, and faster, and they have been successful in that regard. However, they have also become afflicted by malicious actors who seek to sow division, undermine trust in democracy and public institutions, and mislead people into believing, acting on, and sharing false, misleading, sensationalized, or unverified material.

While content moderation is a critical piece of technology platforms' approach to addressing the reach of disinformation, other considerations are also important. For example, technology researchers have contributed evidence that platform design optimizes the spread of disinformation even when it is challenged.[4] Researchers have also found that decentralized communication, which platforms are designed to facilitate, can also amplify disinformation.[5] Thus, a key challenge for technology companies is that a certain amount of disinformation may be endemic.

In the scenario that follows, a coalition of civil rights organizations organizes a virtual voter registration drive on social media platforms about a month before the presidential election. The event is marketed heavily toward young and minority non-voters across the United States. The voter registration event is disrupted, and a brigade of accounts which cannot be attributed engage in a coordinated effort to scapegoat platforms and government for the disruption.

Contextual Note: The voter registration drive is considered a large scale, high impact event. In this scenario, virtual voter registration events organized by civil society groups between August and October 2020 coincided with a significant influx of voter registration applications, including 1.5 million new applications across 18 states. Voter registration deadlines fall 30 days before the election in most states. YouAndMe is a popular social media platform with a global usership of over one billion. The site has been criticized because the CEO is a key contributor to the incumbent's campaign.

4, 5 P. M. Krafft & Joan Donovan (2020) Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign, Political Communication, 37:2, 194-214, DOI: 10.1080/10584609.2019.1686094

- *Inject 1:* Approximately 35 days before the Presidential election, days before most state deadlines for voter registration, a coalition of civil rights organizations, social justice advocacy organizations, celebrities, and former US presidents is set to hold a virtual voter registration event.
- *Inject 2:* As the event proceeds on the social media site and application YouAndMe, over 20 million attendees tune in virtually. Nearly all attendees are US users. Midway through the event, US-based Android users are dropped from the event and cannot reconnect. An error alert indicates to users who were dropped that the site's server is down.
- *Inject 3:* As the event continues to stream, additional disruptions occur. Former US presidents and celebrities are interrupted by intermittent server issues. Shortly thereafter, the application suffers an outage and the event is completely disrupted.
- *Inject 4:* Due to the disruption, the event can not proceed. Shortly after, the President issues several posts on social media, including an inflammatory post suggesting there will be widespread electoral fraud due to mail-in voting.
- *Inject 5:* In the following days, members of the event organizing committee talk to YouAndMe to express frustration at the disruption. A celebrity who participated in the event questions the feasibility of the President's post given server issues in the same timeframe in which the event was disrupted.
- *Inject 6:* After the celebrity's comments, a brigade of accounts offers alternative explanations for the President's reaction. A conspiracy emerges: The US Government requested YouAndMe to disrupt the event due to its perception that voter registration is a threat to the White House incumbent's chances at electoral victory. These accounts cannot conclusively be attributed by the social media platforms as inauthentic, nor do these accounts appear to violate the site's terms of service, and so they are not taken down.

DISCUSSION QUESTIONS: TECHNOLOGY PLATFORMS

1. What initial actions would your company take to restore the event or allow it proceed?
2. What are possible explanations for server issues causing a site crash while certain accounts can post? How would your company explain this situation to users?
3. A key driver of disinformation in this scenario is discontent among users that the site deliberately disrupted an event marketed heavily toward young and minority nonvoters. How would your company aim to assuage concerns that it stymied voter registration on behalf of the government?
4. In injects 4 and 5 of the exercise, highly visible social media users, including elected officials with verified accounts, are involved in spreading unverified information. Would your company work to moderate these posts? If so, how? If not, why?
5. More generally, what considerations drive decisions about whether and how to moderate false content from highly visible public figures or heads of state? How does your company think about how to manage concerns from users that public figures receive preferential treatment when violating terms of service?

6. What, in your estimation, are the most effective countermeasures a platform can implement against disinformation? Which of these might be best suited to these circumstances? To what degree does publicly exposing inauthenticity when it's discovered appear to change the propensity of users to engage with false and inauthentic content in the future? If so, what sorts of changes? If not, to what do you attribute the lack of change?

DISCUSSION QUESTIONS: PROFESSIONAL MEDIA ORGANIZATIONS

1. What would your organization consider to be the best way to report the story that unfolds in the scenario? What factors would you consider when determining how to frame the events and the crux of the story?
2. What best practices in conspiracy theory reporting might inform your organization's approach on this issue? Are there techniques that can be used to report on the facts without giving further oxygen to the conspiracy theories being spread online?
3. When public figures are sharing unquestionably false narratives, how do you determine who is an authority and who you will quote? What experts, observers, or commentators might you or your organization select to provide context and background on this issue for viewers and readers?

DISCUSSION QUESTIONS: UNITED STATES INTELLIGENCE COMMUNITY

1. How could the USIC and/or US Cyber Command (CYBERCOM) assist technology companies with a response as an attack proceeds? For example, after the first indications of an attack, are there avenues by which the USIC or CYBERCOM could escalate a response as a means of quelling the attack?
2. If your organization became aware of a plan by a foreign actor to disrupt the event, how would that information be communicated to the event organizers, the hosting platform, and the public? What courses of action might you recommend?
3. Would the USIC defer to platforms to make a determination about whether to publicize information about the cause of the disruption? Would it allow the platform to make further determinations about what information to publicize?
4. At what point might your agency break protocol to publicly correct false information? Would the level of public interest and/or topic affect this decision?

EXERCISE 3: HACK AND LEAK (PROFESSIONAL MEDIA ORGANIZATIONS)

EXERCISE 3. HACK AND LEAK

(PROFESSIONAL MEDIA ORGANIZATIONS)

SINCE DISINFORMATION has become a foremost topic in public life, the essential task of news organizations has shifted. Previously, journalists worked to convey an objective orientation to facts and truth in the course of their reporting. Today's environment requires that journalists engage with falsehoods, conspiracy theories, and harmful speech. Certain best practices have emerged, including prebunking, debunking, and fact checking. While important, these practices often do not curtail the reach of disinformation. This state of play gives rise to several important questions about how media should adapt to the challenges of this moment, and in particular, how news organizations should report on and engage with disinformation to avoid reinforcing it.

This challenge is compounded by several other complex problems. First, Americans report waning trust in established and traditional media. A January 2020 Pew Research Center report indicates that Americans have grown to perceive established media sources as alienating, while overall trust in those same sources has decreased over the past five years.[6] Across the political spectrum, media professionals regularly contend with accusations of bias, which can lead the public to perceive news as inherently biased. This can in turn cause people to become dismissive of traditional media altogether, or seek out information which confirms their existing beliefs.

Second, disinformation is often optimized for virality and readily monetized. False and sensationalized stories, particularly those on high interest topics, facilitate significant uptick in traffic and engagement.

Finally, today's news environment is difficult. Journalists and reporters have found themselves the subject of politically motivated attacks, including allegations that legitimate reporting is "fake news." Journalists must weigh a wide range of considerations as they fact-check, investigate, vet sources, and observe best practices and journalistic ethics in a highly competitive, around-the-clock news cycle. The ubiquity of disinformation complicates their work.

In the three-part scenario that follows, a major print publication exclusive indicates that the email server of the election commission in a swing state has been infiltrated by an unknown actor. The state is expected to play a key role in deciding the election, calling into question the state's ability to conduct the electoral process with full integrity on November 3. The scenario explores the role of media in promoting competing narratives about the implications of what occurred.

6 Pew Research Center, January, 2020, " Media Polarization and the 2020 Election: A Nation Divided"

PART I

- *Inject 1:* On October 23, 2020, a major print publication, *the Metropolis Times,* runs an exclusive with a headline which reads: "STATE ELECTION COMMISSION HACK: VOTER ROLLS APPEAR COMPROMISED IN DEVASTATING ATTACK".

- *Inject 2:* The exclusive indicates that the email server for top officials in the state election commission has been infiltrated by an unknown actor. This reporting further conveys that emails obtained in the intrusion contain indications that the commission *might* have lost access to its electronic electoral rolls following the alleged intrusion.

- *Inject 3:* The emails in question capture an escalating sense of panic among state commission staff, volunteers, and officials who were experiencing difficulty accessing voter databases and are unable to determine the problem, leaving *Metropolis Times* reporters and quoted experts to infer that the lack of access was caused by the hackers.

- *Inject 4:* The piece goes on to indicate that its source for the exclusive was an individual who purports to be one of the hackers, and that this individual provided the publication with emails, which appear to be authentic, that appear in the reporting. State officials could not be reached for comment on the matter, calling into question the state's ability to conduct the electoral process with full integrity on November 3.

- *Inject 5*: Almost immediately after the *Metropolis Times* story is published, thousands of accounts across social media platforms begin commenting on it, resharing it, and engaging with reporters on its substance. Overwhelmingly, accounts engaging with this topic reinforce the narrative from the *Metropolis Times* piece that the state has in fact lost access to its voter rolls; the commission won't be able to retrieve the rolls before Election Day; and if the rolls are retrieved, their integrity will most certainly be compromised. Threat intelligence and other telemetry are inconclusive as to the authenticity of this online engagement.

- *Inject 6*: Although a few conclusively inauthentic accounts and posts are taken down, the vast majority are left untouched. The content of the publication's coverage becomes a trending topic for several days and is driven largely by user engagement and coverage by mainstream print and broadcast outlets.

PART II

- *Inject 7*: In an attempt to correct the record, on October 28, the state's chief elections officer holds a press conference to confirm the email intrusion but deny the *Metropolis Times* reporting on the voter rolls. State officials reassure the public that they indeed have access to the voter rolls and are prepared to administer voting for the general election on schedule and with full integrity. Furthermore, state officials cite protocols which require that they confer with DHS and FBI as an explanation for their delay in denying the reporting.
- *Inject 8:* As mainstream publications continue to cover this news, platforms again see a significant increase in authentic and inauthentic user behavior advancing the false narrative about the state's voter rolls suggesting the "election is rigged" and therefore that "election outcome is likely to be illegitimate."

PART III

- *Inject 9:* Despite an aggressive response from technology companies, inauthentic behavior and content related to *Metropolis Times* reporting continues to dominate online discourse. The following week on election night, vote totals between the two candidates narrow within a small margin, prompting state officials to conduct a recount. State officials indicate that the results of the recount may not be available for up to a week.
- *Inject 10:* In the intervening week, thousands of social media users report that they were refused ballots due to not having been registered to vote. Additionally, hundreds report having been denied a provisional ballot. While users reference the *Metropolis Times*-reported intrusion as potential explanation, outrage, concern, and confusion erupts among the public.

DISCUSSION QUESTIONS: PROFESSIONAL MEDIA ORGANIZATIONS

1. Would you or your organization have made the decision to publish this piece, as the Metropolis Times did? Why or why not?
2. Would your organization publish illicitly obtained (hacked) material or publish quotes or commentary about the material by the hacker? What considerations would guide your decision making?
3. What courses of action might your organization consider to address false narratives, conspiracy theories, and other harmful false information resulting from the exclusive and subsequent reporting? Similarly, how could Metropolis Times approach issuing a correction to this story without inadvertently reinforcing false or misleading information?
4. Does your organization observe a set of best practices for vetting sources and the material they provide?
5. In this scenario, did you observe that certain journalistic practices contributed to the spread of false information? If so, enumerate them and detail how they could be modified to minimize the spread of disinformation.

6. How does your organization approach framing stories like the Metropolis Times exclusive for online audiences? What efforts might you be required to undertake to ensure stories related to the election are shared with due context about sources, the material provided by sources, and potential implications of the reporting for the election?

DISCUSSION QUESTIONS: STATE AND LOCAL ELECTION OFFICIALS

1. Can you describe how your jurisdiction would coordinate with the Metropolis Times, other national media, or local media in the days and weeks after the exclusive? Would any of these relationships predate the exclusive?
2. In Inject 7 of the scenario, the state's chief election officer holds a press conference to correct the record. Would your organization or jurisdiction follow the same course of action? What other options or additional steps might your organization or jurisdiction consider to fact check and debunk false information resulting from the exclusive?
3. What responsibilities does the media have to state and local election officials when reporting on potentially explosive election-related stories that are likely to be targets of disinformation? Should a protocol exist between state officials and members of major media outlets that enables state officials to receive advanced notice on certain types of stories so as to minimize the harm that might occur?

DISCUSSION QUESTIONS: UNITED STATES INTELLIGENCE COMMUNITY

1. What role (if any) would the USIC play in investigating what occurred in the scenario?
2. If your organization became aware of foreign involvement in the scenario's events, how, when, and to whom would the information be communicated?
3. What responsibility would the USIC have to publicly correct any of the false narratives that arise throughout the scenario?

DISCUSSION QUESTIONS: TECHNOLOGY PLATFORMS

1. In Inject 6, in response to the flood of false information being shared on social media, "a few conclusively inauthentic accounts and posts are taken down, [but] the vast majority are left untouched." How would your organization handle the situation at this point in the scenario?
2. In Inject 8, the scenario notes a renewed uptick in authentic and inauthentic activity related to the reporting. Would your company's actions change at this juncture, given the significance of the disinformation to the election? Why or why not?

EXERCISE 4: VOTE TALLY DISCREPANCY: UNITED STATES INTELLIGENCE COMMUNITY

EXERCISE 4: VOTE TALLY DISCREPANCY

(UNITED STATES INTELLIGENCE COMMUNITY)

The United States Intelligence Community (USIC) is tasked with evaluating cybersecurity threats to the election and synthesizing the national security implications of foreign influence on US elections. Entities such as the Global Engagement Center (GEC) within the US Department of State, the Elections Threat Executive (ETE) within the Office of the Director of National Intelligence (ODNI), and the Foreign Influence Task Forces within both the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have dedicated significant resources to understanding and countering disinformation operations intended to influence US voters.

The USIC is inherently an apolitical group of agencies whose work, in large part, is conducted in secrecy. These factors make it all the more imperative that the USIC develops plans and practices to monitor and disrupt potentially damaging influence operations in a coordinated manner without violating US surveillance frameworks or the Constitution. As technology evolves, the USIC has to stay ahead of the sophisticated techniques used to create and disseminate false and misleading information, much of which can have grave consequences for those targeted.

In the scenario that follows, the Presidential election is disrupted by reports of a cyber intrusion by a foreign adversary. The USIC must determine whether it will make its findings about the intrusion public, and to what extent, in light of the false narratives that result.

- *Inject 1*: Approximately two hours after voting in the eastern United States has concluded, county election offices in several states report to their respective officials that there are significant discrepancies in vote tallies. Consistently, vote tallies recorded by memory cards in county voting machines are reported between 25-40% higher than vote totals reported electronically.
- *Inject 2*: In four states, the winner of the presidential race has already been declared and announced, although votes have not yet been certified. Seven other states affected by the same discrepancy decline to announce a winner, indicating publicly that additional time is needed to properly count votes cast.
- *Inject 3:* Upon an investigation, several USIC agencies independently find that a foreign adversary is responsible for the disruption. It appears a foreign actor successfully infiltrated both the SFTP server[7] and the firewall which protects it, intercepted vote tallies as they were transmitted, and transmitted false vote tallies to county election offices in real time. In effect, it appears that this infiltration aimed to assist the challenger in the presidential race, a member of the Peoples' Victory Party.

7 Elections jurisdictions across the United States operate an electronic system for transferring voter data to county election offices where votes are often tabulated. An SFTP (Secure File Transfer Protocol) facilitates file sharing between polling locations, local precincts, and county election offices. The server itself may or may not be encrypted, network connected, or accessible only to authorized users. Center for Internet Security. (2018). A Handbook for Elections Infrastructure Security. East Greenbush, New York: Author. (The content of this publication is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA-4.0).

- *Inject 4:* In the days after the election, as intelligence and other telemetry become available, professional news organizations begin to report that state officials have indicated to them "off the record" that a cyber intrusion disrupted the election. News organizations host computer scientists and election experts, who indicate that "our elections are easy to manipulate" and that it is "very likely" that election systems were infiltrated as reported.
- *Inject 5*: On social media, varying narratives and conspiracies about the cause of the disruption begin to circulate. A primary conspiracy indicates that the attack was orchestrated by US allies hoping to oust the White House incumbent.
- *Inject 6*: As this narrative aggregates into trending activity on social media, coverage by professional media organizations continues, the White House incumbent begins to use social media platforms to publicize inaccurate theories about the cause of the intrusion. Many cite the idea that US allies carried out the attack to oust the White House incumbent.
- *Inject 7:* As this situation continues to intensify, USIC agencies are under pressure from congressional leaders to make its findings public; likewise, state election officials are under pressure to explain what systems they will use to conduct the election again, including printing scores of hand-marked paper ballots.

DISCUSSION QUESTIONS: INTELLIGENCE COMMUNITY

1. At what point in this scenario would the USIC agree to make its findings about the intrusion public?
2. What extent of findings would be publicized, if any?
3. What information would be shared with state and local election officials?
4. What considerations would drive your agency's thinking about what information is appropriate for publicization? Does this reflect the current protocols across the USIC?
5. At what point, if any, would the USIC respond publicly to address this situation or the false narratives therein?

DISCUSSION QUESTIONS: STATE AND LOCAL ELECTION OFFICIALS

1. What responsibility would your organization have to address the true and false information circulating about what occurred in the scenario?
2. Does your organization already have established lines of communication with USIC points of contact to help manage the cascading effects of an incident such as the one in the scenario?
3. What are potential causes of a discrepancy between manually and electronically reported vote totals? What measures are in place in your jurisdiction to reconcile these differences? Do you have a plan to communicate about a potential discrepancy, and measures to reconcile them, to the public?

4. Would your jurisdiction declare electoral outcomes before receiving physical memory cards from county voting machines?
5. How quickly could your state produce hand-marked paper ballots in the machines that are unreliable?
6. Could an infiltration of the SFTP server and firewall be rectified as voting proceeds?

DISCUSSION QUESTIONS: TECHNOLOGY PLATFORMS

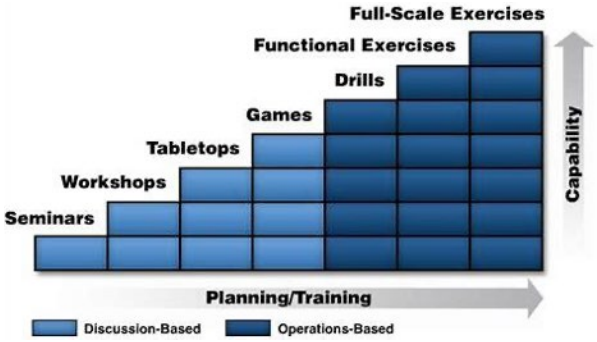
1. How would your company work to stem the spread of false information about the intrusion? What options are available to curtail the spread of false information, and how would you decide between them?
2. What would you prioritize when considering how to limit the spread of false information, i.e. violations of terms of service, apparent inauthenticity in account behavior, or other telemetry?
3. What information could and would your company make public about coordinated behavior or inauthentic content on the site as this event unfolds, and in its aftermath? Would this information be delivered publicly or on a more individualized basis?
4. On Election Night, what steps might your company take to manage the spread of unverified content and claims about the election, if any? If your company would not take such action, can you describe why?

DISCUSSION QUESTIONS: PROFESSIONAL MEDIA ORGANIZATIONS

1. In this scenario, disinformation spawns from the idea that a foreign ally staged the attack to hinder the White House incumbent's chances of electoral victory. How might your organization consider engaging with this idea before becoming aware that it is false? Would this change after becoming aware that it is false?
2. What officials or technical experts might your organization choose to elevate to provide accurate information about the election? What proof, if any, might your organization request they provide before speaking to the public?
3. Can you describe how you or your organization may consider fact checking false information resulting from the intrusion?

APPENDIX A: CONDUCTING A STRUCTURED TTX

TABLETOP EXERCISES (TTXs) encompass one of several categories of exercises meant to explore, test, and strengthen an organization's plans and capacity to address potential adverse situations. The benefit of TTXs is that they are low-cost, low stakes opportunities for participants to talk through difficult scenarios, identify areas for improvement, and implement changes before an actual event takes place.



Credit: FEMA

TTXs are effective for planned events (like an upcoming election), unplanned events (like a terrorist attack), and potential or anticipated events (like protests in response to a significant national occurrence). The issue of disinformation spans each of these types of events, and conducting a structured TTX based on a realistic scenario can be an effective way to prepare for potential impacts of disinformation.

Following are general guidelines for conducting a structured TTX using the scenario narratives provided.

PARTICIPANTS

Assemble a set of individuals with differing roles, perspectives, and responsibilities in relation to addressing disinformation within your industry or organization. TTXs generally work best when there is a range of participants.

The term "participant" encompasses many groups of people, not just those playing in the exercise. Groups of participants generally involved in TTXs, and their respective roles and responsibilities, are as follows:

- **Facilitators**: Facilitators ensure that the TTX is conducted smoothly and in an organized manner. They explain the rules and parameters that will guide the exercise, and ensure that all participants have what they need to perform their roles. Facilitators also provide scenario updates (injects), moderate discussions, and answer questions as required.
- **Players**: Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated scenario.
- **Observers**: Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Evaluators**: Evaluators are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions align to plans, policies, and procedures.

TTX BEST PRACTICES

TTX best practices include the following recommendations:

- The exercise should be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected and encouraged.
- Players are encouraged to respond to the scenario using their knowledge of existing plans and capabilities, and insights derived from training.
- It should be made clear that decisions are not precedent-setting and may not reflect the organization's final position on a given issue. The exercise is an opportunity to discuss and present multiple options and possible solutions.
- Participants should assume cooperation and support from other responders and agencies.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and recovery efforts. Problem-solving efforts should be the focus.
- Situation updates, written materials, and resources provided are the basis for discussion; there are no situational or surprise injects.

EXERCISE ASSUMPTIONS AND ARTIFICIALITIES

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively impact their participation. Participants are encouraged to acknowledge that:

- The scenarios are plausible, and events occur in the order they are presented.
- Some adversary events that would occur in real life are not presented as scenario injects.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.
- The scenario is not derived from current intelligence.

EXERCISE DEBRIEF AND EVALUATION

The facilitator(s) will lead a debrief with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. Players can also be asked to complete participant feedback forms. The participant feedback forms, coupled with facilitator observations and notes, should be used to evaluate the exercise and compile an after-action report (AAR).

ADDITIONAL TTX RESOURCES

For additional information on conducting a TTX, please see the following link, provided by Ready.gov: https://www.ready.gov/business/testing/exercises

APPENDIX B: ADDITIONAL RESOURCES

Polygraph.info: Polygraph.info is a fact-checking website produced by Voice of America (VOA) and Radio Free Europe/Radio Liberty. The website serves as a resource for verifying the increasing volume of disinformation and misinformation being distributed and shared globally. A similar website in the Russian language can be found at factograph.info.

First Draft News: First Draft News offers training courses for journalists covering challenging and high interest topics that are accompanied by disinformation.

#TrustedInfo2020 (NASS): The National Association of Secretaries of State (NASS) has launched #TrustedInfo2020, an educational effort to promote election officials as the trusted sources of election information. By driving voters directly to election officials' websites and social media pages, NASS hopes to ensure voters are getting accurate election information and cut down on the misinformation and disinformation that can surround elections. #TrustedInfo2020 aims to highlight state and local election officials as the credible, verified sources for election information.

Election Integrity Partnership (Stanford Internet Observatory): The Election Integrity Partnership, based at the Stanford Internet Observatory, is a coalition of research entities working to support real-time information sharing on threats to the election.

Election Security Resource Library (DHS/CISA): The Cybersecurity and Infrastructure Security Agency (CISA) Election Security Resource Library provides a portfolio of resources for state and local governments to secure election-related assets from cyber and physical risks. CISA also offers a number of training opportunities for election infrastructure security assistance.

Defending Digital Democratic Project (DP3) (Harvard Belfer Center): The Harvard Belfer Center's Defending Digital Democratic Project (DP3) offers a wide array of resources for state and local election officials. The project offers playbooks for incident training and assessment, and also offers a national training tour for state and local officials in TTX format.

How Society Can Combat Misinformation and Hate Speech Without Making it Worse (Technology and Social Change Research Project, Harvard University): Joan Donavan, Research Director of the Harvard Kennedy School's Shorenstein Center on Media, Politics, and Public Policy, provides recommendations to guide media's engagement with disinformation.

Protected Voices (FBI, ODNI, DHS/CISA): The Protected Voices initiative provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats. Protected Voices resources include information and guidance from the FBI, the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI).

#Protect2020 (DHS/CISA): #PROTECT2020 is a national call to action initiated by CISA, the lead federal agency responsible for national election security, to enhance the integrity and resilience of the Nation's election infrastructure, and ensure the confidentiality, truthfulness, and accuracy of the free and fair elections necessary for our American way of life.

Combatting Targeted Disinformation Campaigns: A whole-of-society issue (DHS/Interagency Partners): This framework was developed as a part of the 2019 Public-Private Analytic Exchange Program. Its recommendations include actions that a variety of stakeholders can take to combat disinformation campaigns.

Combating Foreign Influence (FBI): In the fall of 2017, Director Christopher Wray established the Foreign Influence Task Force (FITF) to identify and counteract malign foreign influence operations targeting the United States. The FITF consists of representatives from the FBI's Counterintelligence, Cyber, Criminal, and Counterterrorism Divisions, and the task force also coordinates with other FBI divisions as needed. Task force personnel work closely with other US government agencies and international partners concerned about foreign influence efforts aimed at their countries.

Elections Cyber Tabletop in a Box (DHS/CISA): CISA developed the Elections Cyber Tabletop Exercise Package (commonly referred to as "tabletop in a box") as a resource for state, local, and private sector partners. The package includes template exercise objectives, scenario, and discussion questions, as well as a collection of cybersecurity references and resources. Partners can use the exercise package to initiate discussions within their organizations about their ability to address the potential threats to the election infrastructure.

Digital Forensic Research Lab (The Atlantic Council): The mission of the DFRL is to identify, expose, and explain disinformation where and when it occurs using open source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space.