Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

2020 Election Series: Foreign Threats to the 2020 Election

October 2020

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

2020 Election Series: Overview of Foreign Threats to the 2020 Election

Introduction

This white paper is the second in an election-focused series that will examine the potential threats associated with the current election landscape. This paper will provide a detailed overview of the foreign threats to the 2020 U.S. Presidential election emanating from three primary adversaries: Russia, China, and Iran. Russia successfully conducted an interference campaign during the 2016 U.S. Presidential election, and current evidence suggests similar efforts are underway for the current election. China has been highlighted by U.S. officials as another potential threat to election integrity, as has Iran.

These (and likely other) foreign countries seek to utilize a variety of approaches in pursuit of a variety of outcomes related to the 2020 election. Such approaches are generally cyber-based, to include spreading misinformation and disinformation online, hacking of candidates/campaigns, and even potentially tampering with election-related systems (such as voting machines) to change the counting of votes. Regarding these countries' desired outcomes, foreign countries may seek to boost a candidate deemed most favorable to the country's own interests, or, alternatively, may seek to disrupt the electoral process as a whole, sowing discord and distrust among the American electorate. However, each of the three primary adversaries (Russia, China, and Iran), have unique goals regarding the 2020 election, and a variety of capabilities to deploy in pursuit of their goals.

Case Study: Russian Election Interference in 2016

As noted in the previous Election Series white paper, Russia's efforts to interfere in the 2016 presidential election were described by a bipartisan U.S. Senate Committee as "an aggressive, multifaceted effort" that included the targeting of presidential campaign members, along with hacking attempts and information operations.[1] Although foreign nation-states (to include Russia) have engaged in overt and covert attempts to influence U.S. elections prior to 2016, Russia's efforts in 2016 represent an unprecedented level of election interference in the United States. As such, it is difficult to summarize the whole of their efforts in a concise manner. Still, some key points are important to note in order to understand the foreign threat landscape facing the current presidential election.

Russia's 2016 election interference was heavily dependent on influence operations, to include misinformation, disinformation, and amplifying a variety of narratives (occasionally playing both sides of an issue) to drive increased polarization amongst the U.S. electorate. Moreover, intelligence community assessments have asserted that Russia actively promoted the candidacy of Donald Trump, who ultimately won the 2016 election and became president.[2] Russia's efforts included social media posts that boosted then-candidate Trump, as well as Green Party candidate Jill Stein (with the assumption that votes for Stein would come at the expense of Democratic candidate Hillary Clinton). Russian social media efforts also disparaged Hillary Clinton, and sought to suppress voter turnout (as lower turnout generally benefits republicans).[3] Russian efforts

also specifically targeted African-Americans, with geo-targeting of ads in predominantly African-American areas and an emphasis on fake accounts that focused on racial issues and amplified racial tensions.[4] Russia also sought to amplify ongoing debates over "gun rights, veterans issues, patriotism, feminism, and even the movement to have California secede from the US," and "the war in Syria."[3]

Additionally, Russia has engaged in hacking operations directed toward U.S. political campaigns, parties, and related entities, as well as governmental targets and voting infrastructure. In 2019, the Senate Intelligence Committee acknowledged that Russia had targeted election infrastructure in all 50 states – for example, evaluating voting machines for potential cyber vulnerabilities. While the Russian effort was far-reaching, there was no evidence that any votes were altered.[5] Still, Russian actors were "in position" to tamper with voter data in Illinois, and successfully compromised voter registration databases in two counties in Florida.[5,6] Russia-linked hackers were also responsible for the high-profile hacking of the Clinton campaign (particularly the emails of campaign manager John Podesta) and the Democratic National Committee. Credentials gathered in these attacks were also used to access the networks of the Democratic Congressional Campaign Committee.[7] Emails and other documents gathered during these hacks were then distributed to the general public through Wikileaks, who has distributed a number of other hacked/leaked/stolen documents in recent years.

Due to Russia's relative level of success in disrupting and influencing the electoral process during the 2016 election cycle, it is increasingly evident that they are engaging in similar efforts in the lead-up to the 2020 election, which will be discussed in detail below. Moreover, countries such as China and Iran are attempting to mirror Russia's tactics in hopes of achieving similar outcomes.

Russia

Russian interference in the 2020 election is not a hypothetical situation. Evidence of Russian impact to the current election cycle is already apparent. Experts and federal institutions including the Department of Homeland Security have, in recent months, pointed to Russia as "the likely primary covert influence actor and purveyor of disinformation and misinformation within the Homeland," in addition to posing an acute cybersecurity threat.[8]

Motivation

The primary goal of Russia is to increase its own global standing and influence. To do this, they are attempting to weaken the United States and prevent it from being able to present any challenge to Russian objectives. Broadly, this is achieved by dividing and destabilizing the country.[8]

Russian attempts to sway voters have two beneficial effects. Firstly, Russia may succeed in promoting a politician or political party which has pro-Russian policies or views. Conversely, Russia may also seek to dissuade voters from supporting politicians who hold views or support policies that will harm Russia or Russian interests. Russian online actors have attacked or praised multiple presidential candidates in the 2020 election.[8] The CIA has assessed that in both the 2016 and 2020 election, Russia has most likely aimed interference operations at raising now-President Trump's election chances. The FBI director has echoed this assessment.[2] The 2020 assessment was presented in September with moderate confidence, a lower degree of certainty than the 2016

assessment, in part because the intelligence community appears to lack intercepted communications or other direct evidence.[9] Secondly, the successful swaying of voters by an outside country with a particular political agenda serves to undermine national trust in the democratic system. When countries succeed in eroding the trust of voters in U.S. institutions, leaders, and the democratic process, the United States is likely to suffer further divisions and destabilization. Any successful disruption of the electoral process, namely voting, through a variety of potential methods will also contribute to the erosion of national confidence in the democratic process.[10]

Russia is also motivated to aggravate pre-existing tensions in the United States. By amplifying both sides of social and racial issues, a tactic which will be discussed below, Russia can intensify discord and perceived grievances against various individuals, groups, political parties, and institutions.[8] This increasing discord again serves to destabilize the country, strengthening Russia's global influence and lessening the chance of U.S. interference in Russian objectives.[11]

Methods

The methods Russia has utilized thus far in seeking to impact the 2020 election are all cyber in nature. Many documented methods utilized in the 2016 and, to a more limited extent, 2018 election cycles continue to be in use by Russian actors. In 2016 false information on the time, date, and manner of voting in the united states was created and/or amplified by Russian interests.[8] In 2020 so far, Russia has continued to attempt to impact voting in spreading incorrect information on both how to vote as well as the security or vulnerability of ballots.[10] It is possible that as the election gets closer, further attempts will be made to obfuscate correct methods, times, and locations for voting. Decreasing turnout and total number of votes for the 2020 election is also used by Russian actors to further dimmish confidence in the outcome of the election and sow discord. In 2016, Russian influence actors posed as U.S. persons and discouraged African Americans, Native Americans, and other minority voters from participating in that year's election.[8,12]

Swaying individual voters is another method utilized in Russia's campaign to influence the 2020 election. This can be accomplished through media manipulation: bot accounts, proxy websites, social media platforms, and traditional media.[13] Through media manipulation Russia has sought to further inflame preexisting social, political, racial, and cultural divisions.[12] In one instance, Russian actors created a phony website and paid freelance American journalists to write stories.[10] One of the more common ways this is achieved is through the mimicking of target audiences - pretending to be a member of the targeted group. Through this, Russian actors have been able to amplify discord and target specific communities in the United States. Russian online influence actors have been found engaging with a wide array of socio-political issues relevant to the 2020 elections. For example, Russian actors have been found by DHS to have amplified narratives such as U.S. law enforcement ignoring ICE detention requests and releasing an illegal immigrant accused of rape, assaults on supporters and opponents of the President, and portrayals of U.S. law enforcement as racially biased.[8]

During the 2020 election cycle, Russia has also found success in the use of information laundering, planting a narrative with an influential individual who can then amplify that narrative. This enables Russian actors to rely on pre-existing social media platforms, algorithms, followers and new

outlets to boost and spread a specific narrative.[10,13] A recent DHS report describes the tactic as such: "The Russian government promulgates misinformation, threats, and narratives intended to incite panic or animosity among social and political groups." This amplified panic or animosity may serve to persuade some voters to support the candidate Russian actors wish to get elected.[8]

Finally, Russia also has the ability to utilize cyber-espionage and cyber-attacks against the United States. Russian actors have targeted and continue to target critical infrastructure systems, U.S. industry, and all levels of government seeking access to economic, policy, and national security information. DHS believes that it is probable that Russia can conduct cyber-attacks that would result in at least localized effects over hours to days.[8] In 2016, a Russian hacking campaign targeted voting systems in all 50 states. This year, intelligence officials believe that disinformation is the larger threat. However, there is still the potential that Russia may attempt to prevent or delegitimize votes in the United States through an attack on voting booths, locations, or systems.[14] Microsoft reported in September that hackers, including Russian actors, have mounted cyberattacks against hundreds of organizations and people involved in the 2020 election, including the campaigns of both Donald Trump and Joe Biden.[15] Should one or more of these hacking attempts prove successful, a variety of outcomes is possible, including the stealing of sensitive information or the disabling of cyber operations for a campaign or organization.

China

Motivation

National Counterintelligence and Security Center (NCSC) Director William Evanina recently identified the People's Republic of China as one of the principal foreign nation-states attempting to interfere with the 2020 presidential election. Beijing is attempting to influence the outcome and future policy positions. It also hopes to sow discord and erode trust in the electoral process among the American people.[16]

State-sponsored hacking groups with ties to Beijing include "Spamouflage Dragon" and "Zirconium" (or APT31), among others. They use social media to disseminate propaganda. The inundation of news and opinion on social media often makes it difficult to separate legitimate content from propaganda and satire. These groups also use traditional hacking techniques, such as phishing, to target presidential campaigns and obtain potentially damaging material.

Methods

Social media companies are better prepared to stymie propaganda and misinformation/disinformation from groups like Spamouflage Dragon than they were in 2016. But state-sponsored hackers can create "bot" networks rapidly, making counter-efforts difficult. In June 2020, Twitter deleted 24,000 primary accounts from China that published original propaganda, along with 150,000 secondary accounts that shared it.[17] In June and July 2020, Spamouflage Dragon launched a campaign of English-language videos that criticized the current presidential administration's response to COVID-19 and ongoing civil unrest.[18] These videos are usually generated automatically and then shared by bots. Social media providers have attempted to squelch these fake accounts, but new ones will likely take their place, given the ease with which accounts can be created.[19]

The hacking efforts of groups like Zirconium are the first steps of "hack and leak" operations. The groups attempt to phish campaign staff and elected officials to obtain login credentials. The credentials can be used to access systems and search for sensitive and potentially damaging material to spread online. In 2016, Russian hackers used Wikileaks to distribute e-mails stolen from Hillary Clinton's presidential campaign. In June 2020, Vice-President Joe Biden's campaign was unsuccessfully targeted by phishing e-mails from Zirconium.[20] The group also targeted a prominent member of President Donald Trump's campaign, along with members of the international affairs and academic communities. Microsoft reported thousands of attacks between March and September 2020, with nearly 150 compromises.[21]

China's state-sponsored hackers and others will continue to disseminate propaganda and access protected systems through the 2020 Presidential Election. It is virtually impossible to prevent the creation of new accounts that go on to distribute propaganda and misinformation/disinformation. It is equally impossible to prevent phishing e-mails from reaching their intended recipient. If hackers are able to obtain useful material, they may even wait until an opportune time in the election cycle to release it. Like state-sponsored propaganda, the goal is for the story to gain traction among not only users, but the mainstream media. If journalists report on the story, it lends it credibility, even if it is later disproven.[22]

Camille Francois, chief innovation officer of the network analysis company Graphika, recently emphasized that a "whole-of-society" effort is necessary to combat or mitigate the efforts of state-sponsored hackers. There is no feasible way to prevent the initial dissemination of propaganda or the proliferation of phishing e-mails. Social media companies can remove accounts and content after the fact, and cybersecurity firms can perform damage control after a user is phished. Individuals must engage with social media and e-mail with a skeptical eye in order to prevent damage before it occurs.[22]

Iran

Motivation

Iran has attempted to influence American elections for nearly a decade. Tensions with the United States have escalated after its withdrawal from the Joint Comprehensive Plan of Action (JCPOA) in 2018 (also known as the "Iran Nuclear Deal") and the 2020 drone strike on Major General Qasem Soleimani. These efforts include hacking operations and disinformation campaigns. Notably, Microsoft announced that Iran targeted President Trump's reelection campaign in August and September of last year. The attacks followed the announcement of additional sanctions that have economically damaged the country.[23]

Methods

Any attempts to influence the 2020 Presidential Election are part of a larger cyber-warfare and espionage campaign by Tehran. The country maintains a dedicated Cyber Corps, but also, evidently, works with independent hackers. They target a wide range of individuals and institutions, including Iranian citizens at home and abroad, as well as government agencies, academia, think tanks, and nonprofits. Hackers attempt to gain access through traditional techniques such as SQL injections, keyloggers, malware, and trojans. In September 2020, two

Iranian hackers, still at large, were indicted by the United States District Court in Newark, New Jersey for multiple attacks beginning in 2010. Some of these attacks were for personal gain via selling victims' information on the Dark Web. However, some of the stolen information was turned over to Iranian intelligence.[24,25]

The attacks on President Trump's campaign were unsuccessful, but they were part of a broader attempt to identify the e-mail addresses of, according to *The New York Times,* "current and former United States government officials, journalists covering political campaigns and accounts associated with a presidential campaign."[23] The wide scope of Iran's hacking efforts and its antagonistic posture towards the United States will remain unchanged for the immediate future. It is likely that Iran will continue these efforts through the 2020 Presidential Campaign and beyond.

Conclusion

Russia likely represents the greatest foreign threat to the 2020 U.S. election process due to their proven track record of influence and hacking efforts, to include the widespread interference in the 2016 election. China is also uniquely situated to interfere in the 2020 election amidst the COVID-19 pandemic and was singled out by NCSC Director Evanina due to its capabilities and potential intent for interference. Iran also may seek to disrupt the election amidst escalating tensions regarding the U.S. withdrawal from the JCPOA as well as the recent drone strike that killed high-ranking Iranian military official Qasem Soleimani. While this paper has focused on the threats emanating from these three nations, it is possible, or even likely, that similar efforts are underway by other nations, to include North Korea and Cuba, among others. There is significant evidence that interference efforts are underway, although it is still unclear how much influence these and other nations will have on the 2020 election.

While foreign threat actors seek to influence and/or disrupt the United States' electoral process (as detailed throughout this paper), a number of potential domestic threats remain. The next paper in this series will examine domestic threat actors in-depth, with a focus on potential civil disturbance and domestic terrorist activity that could be sparked by a number of potential election outcomes. A subsequent paper will be produced and released after the election has occurred, and will examine the post-election threat landscape. This will include any threat activity that has occurred affecting the election (to include incidents on/around election day), or as a result of the election. Multiple electoral scenarios (to include a contested election) remain possible, and a number of potential threat activities remain as valid concerns.

---

[1] U.S. Senate. (2019, August 18). Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities. Retrieved October 14, 2020, from https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

[2] 'Steady drumbeat of misinformation': FBI chief warns of Russian interference in US elections. (2020, September 17). Retrieved October 15, 2020, from https://www.theguardian.com/us-news/2020/sep/17/misinformation-us-elections-2020-russia

[3] Ward, A. (2018, December 17). 4 main takeaways from new reports on Russia's 2016 election interference. Retrieved October 14, 2020, from https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

[4] Mak, T.(2019, October 08). Senate Report: Russians Used Social Media Mostly To Target Race In 2016. Retrieved October 14, 2020, from https://www.npr.org/2019/10/08/768319934/senate-report-russians-used-used-social-media-mostly-to-target-race-in-2016.

[5] Sanger, D., & Edmondson, C. (2019, July 25). Russia Targeted Election Systems in All 50 States, Report Finds. Retrieved October 14, 2020, from https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.

[6] Parks, M. (2019, May 14). Florida Governor Says Russian Hackers Breached 2 Counties In 2016. Retrieved October 14, 2020, from https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.

[7] Whittaker, Z. (2019, April 18). Mueller report sheds new light on how the Russians hacked the DNC and the Clinton campaign. Retrieved October 14, 2020, from https://techcrunch.com/2019/04/18/mueller-clinton-arizona-hack/.

[8] Homeland Threat Assessment. (2020, October). Retrieved October 15, 2020, from https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

[9] Barnes, J., & Sanger, D. (2020, September 22). C.I.A. Reasserts Putin Is Likely Directing Election Influence Efforts to Aid Trump. Retrieved October 15, 2020, from https://www.nytimes.com/2020/09/22/us/politics/cia-russian-election-interference.html

[10] Myre, G., & Bond, S. (2020, September 29). 'Russia Doesn't Have To Make Fake News': Biggest Election Threat Is Closer To Home. Retrieved October 15, 2020, from https://www.npr.org/2020/09/29/917725209/russia-doesn-t-have-to-make-fake-news-biggest-election-threat-is-closer-to-home

[11] Scott, M. (2020, September 14). Russia is back, wilier than ever - and it's not alone. Retrieved October 15, 2020, from https://www.politico.com/news/2020/09/14/russia-cyberattacks-election-413757

[12] Fischer, S. (2020, September 08). Russia's 2020 election manipulation looks a lot like 2016. Retrieved October 15, 2020, from https://www.axios.com/russia-2020-election-manipulation-disinformation-ebe7a0b9-8dc2-40d8-a29d-17b266b6afea.html

[13] Frenkel, S., & Barnes, J. (2020, September 01). Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say. Retrieved October 15, 2020, from https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html

[14] Dilanian, K. (2020, October 02). U.S. patchwork of state, county election computer networks still vulnerable to cyberattacks. Retrieved October 15, 2020, from https://www.nbcnews.com/politics/2020-election/u-s-patchwork-state-county-election-computer-networks-still-vulnerable-n1241337

[15] Starks, T. (2020, September 11). Russia, China and Iran trying to hack presidential race, Microsoft says. Retrieved October 15, 2020, from https://www.politico.com/news/2020/09/10/russia-china-iran-cyberhack-2020-election-411853

[16] Office of the Director of National Intelligence. (2020, August 07). Statement by NCSC Director William Evanina: Election Threat Update for the American Public. Retrieved October 12, 2020, from

https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[17] Koetsier, J. (2020, June 12). Twitter Catches 182,000 Propaganda Accounts For China, Russia, Turkey. Retrieved October 12, 2020, from https://www.forbes.com/sites/johnkoetsier/2020/06/12/182000-twitter-propaganda-accounts-for-china-russia-turkey-caught/#37859a855950.

[18] Eib, C.S., Francois, C., Nimmo, B., & Ronzaud, L. (2020, August). Spamouflage Dragon Goes to America. Retrieved October 12, 2020, from https://public-assets.graphika.com/reports/graphika_report_spamouflage_dragon_goes_to_america.pdf.

[19] Google Threat Analysis Group. (2020, August 05). TAG Bulletin: Q2 2020. Retrieved October 12, 2020, from https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/.

[20] Zhang, P. (2020, June 15). China-backed Hackers Target Biden Campaign in Early Sign of 2020 Election Interference. Retrieved October 12, 2020, from https://www.voanews.com/usa/us-politics/china-backed-hackers-target-biden-campaign-early-sign-2020-election-interference.

[21] Burt, T. (2020, September 10). New Cyberattacks Targeting U.S. Elections. Retrieved October 12, 2020, from https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.

[22] Ng, A. (2020, October 09). How Social Networks are Preparing for a Potential October Hack-and-Leak. Retrieved October 12, 2020, from https://www.cnet.com/news/how-tech-platforms-are-preparing-for-a-potential-october-hack-and-leak/.

[23] Perlroth, N. & Sanger, D. (2020, September 18). Iranian Hackers Target Trump Campaign as Threats to 2020 Mount. Retrieved October 14, 2020, from https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html.

[24] Cimpanu, C. (2020, September 16). US Charges Two Iranian Hackers for Years-Long Cyber-Espionage, Cybercrime Spree. Retrieved October 14, 2020, from https://www.zdnet.com/article/us-charges-two-iranian-hackers-for-years-long-cyber-espionage-cybercrime-spree/.

[25] U.S. District Court, District of New Jersey. (2020, September 15). United States of America vs. Hooman Heidarian, a/k/a "Neo" and Mehdi Farhadi, a/k/a "Mehdi Mahdavi." Retrieved October 14, 2020, from https://www.documentcloud.org/documents/7211914-Heidarian-and-Farhadi-indictment.html.