Risk Mitigation Consulting Inc.

*Intelligence and Analysis Division*

# WHITE PAPER SERIES

## 2020 Election Series: Overview of Foreign and Domestic Threats to the 2020 Election

September 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 and Domestic Threats to the 2020 Election

## Introduction

The 2020 U.S. presidential election will be held on Tuesday 03 November 2020, amidst heightened political polarization, the global COVID-19 pandemic, and widespread civil rights protests under the Black Lives Matter movement. Incumbent President Donald Trump (a Republican) is set to face off against former Vice President Joe Biden, who is running on the Democratic Party ticket. The race also features a number of third-party candidates. This complex situation is likely conducive to a variety of threat actors, both foreign and domestic. The election is already attracting foreign interference from adversarial nations such as Russia, although the threat from other countries (to include China and Iran) remains a concern. Conversely, recent protest activity throughout the U.S. has escalated to the point of civil disturbance, and a number of recent domestic terror attacks have been politically motivated.

This white paper is the first in an election-focused series that will examine the potential threats associated with the current election landscape. This paper will provide a top-level overview of the threats from foreign and domestic threat actors, while future papers will examine these threat actors and their activities in-depth.

## Threats to Past Elections

Per the National Counterintelligence and Security Center (NCSC) National Counterintelligence Strategy of the United States for 2020-2022, "foreign intelligence entities are conducting influence campaigns in the United States to undermine confidence in our democratic institutions and processes, sow divisions in our society, exert leverage over the United States and weaken our alliances."[1] While these influence campaigns may occur at any point in time, they are particularly prominent around major elections. Foreign countries may seek to promote a particular candidate over another, or they may simply seek to exploit the electoral process to promote discord among the citizenry and distrust in U.S. institutions.

Foreign actors have a long history of seeking to interfere in U.S. elections, with modern efforts by nation-states beginning in the wake of World War II and continuing throughout the Cold War. These interference efforts were largely conducted by Russia, the U.S.'s primary geopolitical foe during that period, and included overt and covert attempts by Russian leaders such as Joseph Stalin and Nikita Khrushchev to support particular U.S. presidential candidates.[2] However, 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.[3]

Electoral politics have also been a source of domestic threats in the past, to include protest activity and civil disturbances. Nominating conventions are frequent targets of protest activity, with occasional escalation. For example, the 1968 Democratic Convention (which occurred amidst tensions regarding the Vietnam War and the recent assassination of Martin Luther King, Jr.) resulted in violent clashes between protestors and police officers.[4] The 2016 Republican National Convention was also met with protests, which occasionally became violent, resulting in the arrests of a number of protestors and injuries to at least 2 police officers.[5] The election of President Barack Obama was met with the emergence of "Tea Party" protests in hundreds of locations throughout the U.S. in early 2009, though such demonstrations remained generally peaceful.[6] President Donald Trump's election and inauguration in 2016 were met with some violent protests, but also peaceful marches such as the "Women's March."[7,8] Protest activities (including protests that become violent) are likely to continue as the 2020 presidential election approaches.

Additionally, domestic extremists motivated by political ideologies may conduct terrorist attacks. In 2017, an outspoken left-wing activist who had volunteered for Senator Bernie Sanders' presidential campaign opened fire on a gathering of Republican Congressmen practicing for an annual baseball game, severely wounding Congressman Steve Scalise, among others.[9] In 2018, an outspoken supporter of President Donald Trump attempted to mail a number of explosive devices to prominent critics of the President. Fortunately, none of the devices exploded, and many were intercepted in-transit due to the high-profile nature of the intended recipients.[10] While neither of these individuals are inherently representative of those who hold similar political views, strong political views are one factor that can motivate individuals to commit violent acts.

## Foreign Threats

In a statement issued in early August 2020, the NCSC Director William Evanina outlined the three primary foreign nation-states attempting to interfere with the 2020 presidential election: Russia, China, and Iran. These "covert and overt" measures are designed to favor certain outcomes of the election, sow discord, erode trust in the electoral process, and shift policy positions.[11]

### *Election Hacking*

"Election Hacking" is an umbrella term that refers to cyber-attacks, phishing, and spreading misinformation/disinformation. Cyber-attacks can take the form of attempts to gain unauthorized access to a network to check for vulnerabilities, steal or destroy information, and/or cause mischief. Phishing occurs when a target is tricked into furnishing his/her login credentials to a malicious actor or entering them into a fraudulent website. The spread of misinformation/disinformation online is a common tactic to sway voter opinion. "Election Hacking" also refers to manipulation of election results over the Internet. Russian hackers attempted to scan and probe all 50 states' electoral system during the 2016 election. While none were able to manipulate results, state-sponsored cyber-attacks are becoming more sophisticated. Efforts to alter election results are expected to continue.[12,13]

### *Misinformation and Disinformation*

Misinformation is information that is untrue but not necessarily intended to be misleading. Misinformation can also potentially be damaging depending on how it is utilized. Social media users may read something that seems true or likely true and share it, such as a rumor about a celebrity or a candidate for office. It may take the form of harmless or even humorous gossip, but it can also have real world consequences. Correcting misinformation can consume valuable time and resources for individuals, companies, and elected officials and/or candidates for office.

Disinformation is untrue, but it is designed to damage and/or undermine its target. For instance, in 1983, a Soviet-backed newspaper published in India asserted that the United States had created HIV/AIDS as a biological weapon. Other Soviet media outlets worldwide repeated the story, and the conspiracy theory was, and still is, adopted by some American citizens.[14,15] Disinformation spreads even faster online, and it is difficult to correct. Foreign nation-states use disinformation against the United States to target elected officials or candidates for office, influence election results, and undermine confidence in the electoral process.

The three primary foreign nation-states that are attempting to interfere with the 2020 presidential election use social media and websites to circulate disinformation. Social media companies have attempted to remove fraudulent accounts created to share misleading memes and propaganda, but they are difficult to contain. There has also been a proliferation of news websites that appear legitimate, but they publish fraudulent or biased content on behalf of a foreign government.[16]

### *Russia*

Despite its past efforts, only by 2016 was Russia able to effectively influence voters through social media, hacking, releasing stolen documents, and circulating misinformation/disinformation.[17] These efforts continue, and they are largely proffered by the Internet Research Agency (IRA), a Kremlin-backed company that uses "bot" accounts, memes, and fraudulent news sites. The IRA and Russian intelligence services use these sites to circumvent social media companies' monitoring. The sites disseminate information and viewpoints designed to sway voters, some of whom will share their content. This "information laundering" is difficult to detect or prevent. The IRA has even recruited American freelancers to write for these sites.[16]

Since 2016, Russia's Main Intelligence Directorate of the General Staff of the Russian Army (GRU) has continued its efforts to hack American defense, energy, and intelligence systems.[18] In May 2020, the National Security Agency (NSA) publicly accused the GRU of hacking e-mail servers worldwide. This demonstrated that the GRU has the capability and the intention to escalate its efforts in the months leading to the November 2020 election.[19] In early September, suspected state-backed hackers targeted SKDKnickerbocker, a firm advising Joe Biden's campaign. The hackers used phishing to try to obtain login credentials. They were unsuccessful, and the Kremlin has denied any connection.[20] As the election draws closer, the visibility of GRU's attacks on both campaigns has increased. Between 18 August and 3 September 2020, the GRU targeted 6,912 email accounts at 28 organizations. Thus far, none were successful.[21] If the GRU were to successfully obtain the login credentials of a prominent target, it could lead to a second, and possibly worse, release of sensitive documents or damaging information, similar to the 2016 hack of the Democratic National Committee.

### *China*

Director of National Intelligence John Ratcliffe has emphasized the severity of China's threat to national security.[22] Hacking groups with ties to the Chinese government, including "Spamouflage Dragon," have used Twitter, Facebook, YouTube, and TikTok to disseminate propaganda. In August 2019, all but TikTok removed assets linked to the Chinese government. Most were used to target Hong Kong protestors. Similar content had been republished by bot accounts that automatically generate propaganda using an algorithm.[23,24] In June 2020, Spamouflage Dragon published more videos, this time in English and targeting American audiences. The videos attacked the current presidential administration, criticizing the country's response to the COVID-19 pandemic and to the ongoing civil unrest.[25] As a result, from April-June 2020, Google banned over 2,500 YouTube accounts with ties to Spamouflage Dragon.[26] The goals of groups like Spamouflage Dragon are manifold. Twitter itself is banned in China, but some content is targeted at Chinese audiences living abroad. In June 2020, Twitter removed 23,750 accounts that spread original disinformation. The company also removed 150,000 bot accounts that "liked" and retweeted that content. The accounts or sites serve as a mouthpiece for the Chinese government, while the bots propagate its message. In the case of the June 2020 removal, the accounts were praising Beijing's response to the COVID-19 pandemic and denigrating the response of the United States. Some of it, however, is targeted at American audiences. In this case, there were tweets that accused the United States of interfering in the Hong Kong protests while suppressing domestic demonstrations following the May 2020 death of George Floyd. This kind of disinformation is meant to undermine the credibility of the United States government and the faith and confidence of its citizenry.[27,28]

In September 2020, Microsoft reported that state-backed Chinese hackers recently targeted the email accounts of Joe Biden's campaign staff, academics, and the national security establishment. This follows on a Google report from May 2020 that implicated the same hacker group in targeting e-mail accounts within Biden's campaign. None of these hacks were successful.[21] As with the GRU's efforts, hacking e-mail accounts is usually done to obtain information. Sensitive documents or other information uncovered by these types of hacking efforts could potentially be used to disparage a presidential campaign, or could be used to create new disinformation for release at a later date.

### *Iran*

While Iran has traditionally been less of a threat than Russia or China, its cyber capabilities have grown. Their disinformation campaigns have also increased.[29] Since 2011, Iran has leveraged social media accounts and news websites it owns to influence voters in the United States and Britain. In May 2020, Facebook removed 8 networks with ties to the Iranian government and state-run media. According to Reuters, one Tehran-based operation it investigated in 2018 had used more than 70 websites in more than 15 countries posing as local news sites. Iranian disinformation campaigns are designed to propagate the state's point of view on issues abroad, particularly where there is American involvement. As early as 2012, Iranian-backed social media instruments tried to sway a Republican presidential primary. While their efforts have not been as robust as those of Russia in 2016, Tehran has been trying to influence American elections for almost a decade, if not longer.[30]

In October 2019, an Iranian state-backed hacker group dubbed "Phosphorous" attacked 241 e-mail accounts associated with government officials, journalists, and Iranians living abroad. The group also attacked e-mail accounts associated with an unnamed presidential campaign. Four were compromised.[29] Since the October attack, Microsoft has taken control of 155 web domains used by Iranian hackers.[21] From May-June 2020, Iranian hackers targeted the e-mail accounts of campaign officials working for President Donald Trump.[21] In October 2019, Facebook removed 3 networks of fake accounts that were used to disseminate misinformation/disinformation.[29] In June

2019, Twitter also removed 4,779 accounts, the majority of which had ties to the Iranian government.[31] Iranian hackers have targeted corporations, educational institutions, and government agencies. Their attacks have resulted in deleted and stolen data and login credentials.[29] Tensions have escalated between the two after the withdrawal from the Joint Comprehensive Plan of Action in 2018 and the 2020 drone strike on Major General Qasem Soleimani. Tehran will likely continue to support hacking operations and disinformation campaigns to influence the forthcoming election.

## Domestic Threats

Some threats motivated or triggered by the 2020 election may be domestic in nature. The FBI sent out a bulletin to police nation-wide regarding potential domestic threats that may arise due to the 2020 election. They warned that domestic violent extremists "across the ideological spectrum likely will continue to plot against government and election-related targets to express their diverse grievances involving government policies and actions." While every individual has the right to free speech and to gather for peaceful protests, some language and gatherings can escalate to dangerous actions. Recent incidents of civil disturbance and domestic terror activities are generating concerns regarding new or continuing domestic threats.[32]

Looking at the recent history of right-wing and left-wing incidents, some patterns can be identified. Members of both groups include general supporters, those who express verbal support with peaceful or violent intent (to include electronic communication), those who attend protests, rallies or marches, and finally individuals who commit crimes or violent acts in the name of right-wing or left-wing motivations. These incidents can range from property crime to active assailants. Left-wing actors have, in recent events, tended to host large rallies or protests. These protests, while largely peaceful, can result in property damage and incidents of physical confrontations. For example, a recent analysis of nearly 8,000 Black Lives Matter-affiliated protests between 22 May and 26 August 2020 found that 93% of the protests occurred without any reported violence, while 7% included violence(a term defined in the analysis as "demonstrators fighting with police or with counterprotesters" or "demonstrations that resulted in property damage").[33] These protests can also attract malicious actors seeking to take advantage of civil unrest for personal gain. There is a broader history of right-wing actors committing targeted, active assailant attacks. From 2010 to early 2020, the Center for Strategic and International Studies tracked 21 victims killed in left-wing violence in the United States and 117 victims killed in right-wing violence in the United States. Right-wing extremists perpetrated two thirds of the attacks and plots in the United States in 2019 and over 90% between 1 January 2020 and 8 May 2020.[34] Disinformation also appears more likely to be generated and engaged by right-wing actors, though left-wing actors are certainly not immune to disinformation.[35,36]

Rallies, protests, and events hosted by either group all have the potential to draw counter protestors. Counter protests can then clash, creating civil disturbance opportunities. Far-right and far-left networks have both used violence against each other at protests. Recently, some individuals have also pretended to be members of a particular group, commit crimes in that ideology's name, and thereby hope to create retaliation against the group they falsely claim to affiliate with. A number of recently reported incidents have come in the form of right-wing actors committing property crimes under the guise of a left-wing protester.[37]

### *Misinformation and Disinformation*

Misinformation or disinformation can originate abroad or domestically and then, in turn, be utilized by domestic groups or individuals. False information or conspiracy theories, regardless of origin, can result in very real domestic election impacts. The spread of misinformation and disinformation can prompt or inflame individuals. They may change their personal beliefs or opinions, or take action as guided by the misinformation. Recent events have shown that the spreading of misinformation or disinformation can result in actions that can escalate to dangerous situations. One well known example of disinformation resulting in violent action took place during the 2016 presidential election cycle. A loose coalition of individuals and groups, to include "ordinary people, online activists, bots, foreign agents and domestic political operatives" alleged that a pizza restaurant in Washington was harboring young children as sex slaves as part of a child-abuse ring led by Hillary Clinton.[38] These false allegations prompted one man to drive to the restaurant to attempt rescue of captive children. He brought a rifle and handgun with him and fired one shot from the rifle. Though the situation did not result in any harm, it shows how easily disinformation can generate action.[39]

More recently, false allegations regarding a connection between 5G towers and COVID-19 have resulted in property damages as some individuals attempt to damage or destroy various cellphone towers. The Department of Homeland Security remains concerned that further damages may occur and that telecommunications workers may become targets of violent crimes.  Misinformation and disinformation about and relating to the 2020 election is already being spread by foreign and domestic actors. This can very plausibly result in further violent acts, property crimes, or incidents of domestic terrorism in the coming months.[40]

## Conclusion

The full threat landscape surrounding the 2020 presidential election is still unfolding, and foreign and domestic actors alike will likely conduct various forms of threat activities. Foreign nation states will almost certainly continue to conduct influence operation and other forms of malicious cyber activity. Domestically, protest activity (and occasional civil disturbances) will also almost certainly continue given the confluence of the approaching election alongside the continuing COVID-19 pandemic and civil rights-related movements. Moreover, foreign actors will likely continue to propagate misinformation and disinformation, which could potentially influence the results of the election, but could also manifest in violent or destructive acts conducted by domestic actors. While this paper provides a baseline overview of the threats associated with the 2020 election, future papers will examine both foreign and domestic actors (as well as their various threat activities) in greater detail. Additionally, if necessary, future papers will address threat activity associated with unique election-related scenarios, to include a contested election.

[1] Office of the Director of National Intelligence. (2020, January 7). National Counterintelligence Strategy of the United States 2020-2022. Retrieved September 11, 2020, from https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

[2] Michel, C. (2019, October 26). Russia's Long and Mostly Unsuccessful History of Election Interference. Retrieved September 11, 2020, from https://www.politico.com/magazine/story/2019/10/26/russias-long-and-mostly-unsuccessful-history-of-election-interference-229884.

[3] 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 September 11, 2020, from https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

[4] History.com. (2020, March 30). 1968 Democratic Convention. Retrieved September 11, 2020, from https://www.history.com/topics/1960s/1968-democratic-convention.

[5] Krieg, G. (2016, July 20). Cleveland RNC protests: 18 arrested, 2 officers receive minor injuries. Retrieved September 11, 2020, from https://www.cnn.com/2016/07/20/politics/cleveland-republican-convention-protests/index.html.

[6] Jonsson, P. (2009, April 18). Arguing the size of the "tea party" protest. Retrieved September 11, 2020, from https://www.csmonitor.com/USA/2009/0418/p25s03-usgn.html.

[7] CBS News. (2017, January 21). Trump inauguration protest damages parts of downtown Washington. Retrieved September 11, 2020, from https://www.cbsnews.com/news/donald-trump-inauguration-protest-damages-downtown-washington/.

[8] Keneally, M. (2017, January 22). More Than 1 Million Rally at Women's Marches in US and Around World. Retrieved September 11, 2020, from https://abcnews.go.com/Politics/womens-march-heads-washington-day-trumps-inauguration/story?id=44936042.

[9] Pagliery, J.  (2017, June 15). Suspect in congressional shooting was Bernie Sanders supporter, strongly anti-Trump. Retrieved September 11, 2020, from https://www.cnn.com/2017/06/14/homepage2/james-hodgkinson-profile/index.html

[10] Mangan, D. (2019, August 5). 'MAGA Bomber' Cesar Sayoc sentenced to 20 years in prison for trying to kill Trump critics, including Obama, Clinton, Biden, Booker, Harris. Retrieved September 11, 2020, from  https://www.cnbc.com/2019/08/05/cesar-sayoc-sentenced-to-20-years-for-sending-bombs-to-trump-critics.html.

[11] Office of the Director of National Intelligence. (2020, August 7). Statement by NCSC Director William Evanina: Election Threat Update for the American Public. Retrieved September 10, 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.

[12] Martin, A. & Mehrohtra, K. (2019, December 5). What Is Election Hacking, and Can It Change Who Wins? Retrieved September 10, 2020, from https://www.bloomberg.com/news/articles/2019-12-06/what-is-election-hacking-and-can-it-change-who-wins-quicktake.

[13] U.S. Senate. (2019, July 25). Select Committee on Intelligence, United States Senate, on Russian Interference in the 2016 United States Presidential Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views. Retrieved September 11, 2020, from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[14] Gangware, W. & Nemr, C. (2019, March). Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. Retrieved September 14, 2020, from https://www.state.gov/wp-

content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

[15] Heller, J., PhD. (2015, January). Rumors and Realities: Making Sense of HIV/AIDS Conspiracy Narratives and Contemporary Legends. Retrieved September 14, 2020, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4265931/.

[16] Barnes, J.E. & Frenkel, S. (2020, September 1). Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say. Retrieved September 10, 2020, from https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html.

[17] U.S. Department of Justice. (2019, April 18). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Retrieved September 10, 2020, from https://www.justice.gov/storage/report.pdf.

[18] Barnes, J.E. & Sanger, D. (2020, July 28). Russian Intelligence Agencies Push Disinformation on Pandemic. Retrieved September 10, 2020, from https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html.

[19] Barnes, J.E. & Sanger, D. (2020, May 28).U.S. Accuses Russian Military Hackers of Attack on Email Servers. Retrieved September 10, 2020, from https://www.nytimes.com/2020/05/28/us/politics/nsa-russian-hack.html.

[20] Beng, C., Menn, J., Satter, R., & Schectman, J. (2020, September 9). Exclusive: Russian State Hackers Suspected in Targeting Biden Campaign Firm – Sources. Retrieved September 10, 2020, from https://www.reuters.com/article/us-usa-election-cyber-biden-exclusive/exclusive-russian-state-hackers-suspected-in-targeting-biden-campaign-firm-sources-idUSKBN2610I4.

[21] Perlroth, N. & Sanger, D. (2020, September 10). Russian Intelligence Hackers Are Back, Microsoft Warns, Aiming at Officials of Both Parties. Retrieved September 10, 2020, from https://www.msn.com/en-us/news/politics/russian-intelligence-hackers-are-back-microsoft-warns-aiming-at-officials-of-both-parties/ar-BB18UoQZ?ocid=msedgntp.

[22] BBC News. (2020, August 8). US Election 2020: China, Russia and Iran 'Trying to Influence' Vote. Retrieved September 10, 2020, from https://www.bbc.com/news/election-us-2020-53702872.

[23] Eib, C.S., Nimmo, B., & Tamora, L. (2019, September). Cross-Platform Spam Network Targeted Hong Kong Protests. Retrieved September 10, 2020, from https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

[24] Twitter Safety. (2019, August 19). Information Operations Directed at Hong Kong. Retrieved September 10, 2020, from https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html.

[25] Eib, C.S., Francois, C., Nimmo, B., & Ronzaud, L. (2020, August). Spamouflage Dragon Goes to America. Retrieved September 10, 2020, from https://public-assets.graphika.com/reports/graphika_report_spamouflage_dragon_goes_to_america.pdf.

[26] Google Threat Analysis Group. (2020, August 5). TAG Bulletin: Q2 2020. Retrieved September 10, 2020, from https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/.

[27] Conger, K. (2020, June 17). Twitter Removes Chinese Disinformation Campaign. Retrieved September 14, 2020, from https://www.nytimes.com/2020/06/11/technology/twitter-chinese-misinformation.html.

[28] Taylor, J. (2020, June 11). Twitter Deletes 170,000 Accounts Linked to China Influence Campaign. Retrieved September 14, 2020, from https://www.theguardian.com/technology/2020/jun/12/twitter-deletes-170000-accounts-linked-to-china-influence-campaign.

[29] Ranger, S. (2020, January 7). Disk-Wiping Malware, Phishing and Espionage: How Iran's Cyber Attack Capabilities Stack Up. Retrieved September 10, 2020, from https://www.zdnet.com/article/hard-disk-wiping-malware-phishing-and-espionage-how-irans-cyber-capabilities-stack-up/.

[30] Paul, K. & Stubbs, J. (2020, May 5). Facebook Says it Dismantles Disinformation Network Tied to Iran’s State Media. Retrieved September 14, 2020, from https://www.reuters.com/article/us-iran-facebook/facebook-says-it-dismantles-disinformation-network-tied-to-irans-state-media-idUSKBN22H2DK.

[31] Osborne, C. (2019, June 14). Twitter Wipes Out Thousands of Fake Accounts Connected to Iran, Russia. Retrieved September 10, 2020, from https://www.zdnet.com/article/twitter-wipes-out-thousands-of-fake-accounts-connected-to-iran-russia/.

[32] Winter, J. (2020, September 10). FBI warns of increasing extremist threats to the 2020 elections.Retrieved September 11, 2020, from https://www.msn.com/en-us/news/politics/fbi-warns-of-increasing-extremist-threats-to-the-2020-elections/ar-BB18UdXm.

[33] Budryk, Z. (2020, September 03). Over 90 percent of protests this summer were peaceful, report shows. Retrieved September 17, 2020, from https://thehill.com/homenews/state-watch/515082-over-90-percent-of-protests-this-summer-were-peaceful-report-shows.

[34] The Escalating Terrorism Problem in the United States. (2020, June 17). Retrieved September 15, 2020, from https://www.csis.org/analysis/escalating-terrorism-problem-united-states.

[35] Beckett, L. (2020, July 27). Anti-fascists linked to zero murders in the US in 25 years. Retrieved September 11, 2020, from https://www.theguardian.com/world/2020/jul/27/us-rightwing-extremists-attacks-deaths-database-leftwing-antifa.

[36] Gallagher, F., & Bell, B. (2020, April 23). Coronavirus misinformation is widespread, according to new report that calls it an 'infodemic'. Retrieved September 11, 2020, from https://abcnews.go.com/US/coronavirus-misinformation-widespread-report-calls-infodemic/story?id=70249400.

[37] Macfarquhar, N. (2020, May 31). Many Claim Extremists Are Sparking Protest Violence. But Which Extremists? Retrieved September 11, 2020, from https://www.nytimes.com/2020/05/31/us/george-floyd-protests-white-supremacists-antifa.html.

[38] Robb, A. (2017, November 16). Anatomy of a Fake News Scandal. Retrieved September 17, 2020, from https://www.rollingstone.com/feature/anatomy-of-a-fake-news-scandal-125877/.

[39] Kang, C., & Goldman, A. (2016, December 05). In Washington Pizzeria Attack, Fake News Brought Real Guns. Retrieved September 11, 2020, from https://www.nytimes.com/2016/12/05/business/media/comet-ping-pong-pizza-shooting-fake-news-consequences.html.

[40] Margolin, J. (2020, May 16). Feds warn of attacks related to bogus COVID-19 conspiracy theory. Retrieved September 11, 2020, from https://abcnews.go.com/US/feds-warn-attacks-related-bogus-covid-19-conspiracy/story?id=70721145.