HOMELAND SECURITY ADVISORY COUNCIL
INTERIM REPORT OF THE COUNTERING FOREIGN INFLUENCE SUBCOMMITTEE

May 21, 2019

This page is intentionally left blank

This publication is presented on behalf of the Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, under Chair Ali Soufan, Vice Chair Michael Jackson as the ***Interim final report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Kevin McAleenan.

Ali Soufan (Chair)

Michael Jackson (Vice Chair)

This page is intentionally left blank.

COUNTERING FOREIGN INFLUENCE SUBCOMMITTEE

Ali H. Soufan (Chair) Chairman and CEO, The Soufan Group, LLC
Michael P. Jackson (Vice Chair) President and Founder, Firebreak Partners
John R. Allen President, Brookings Institution
Paul Goldenberg President and CEO, Cardinal Point Strategies, LLC
John Magaw Consultant, Domestic and International
Paul Stockton Managing Director, Sonecon LLC
Chad Sweet Co-Founder, The Chertoff Group

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Matt Hayden, Executive Director, Homeland Security Advisory Council
Mike Miron, Deputy Executive Director, Homeland Security Advisory Council
Catherine Fraser, Supervisory CBP Officer, Homeland Security Advisory Council
Colleen Silva, Staff, Homeland Security Advisory Council
Sarahjane Call, Staff**,** Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

EXECUTIVE SUMMARY

The threat of foreign influence (FI) is damaging to the national security of the United States and seeks to undermine our very democracy. Weaponization of information is used as a tool by state and non-state actors alike for different aims and objectives.

While some federal agencies think they are leading the work on countering foreign influence, **no single entity has officially been provided with a mandate to do so. To-date, the United States has no national strategy to counter foreign influence.** The Department leadership can play a leading role in facilitating active coordination between executive and legislative branch activities in relation to countering foreign influence operations. In-addition, **DHS should recommend and support the creation of an interagency organization similar to the NCTC co-lead by DHS and FBI**.

Inside DHS, almost all of the Department operating components have a role to play in countering foreign influence that entails the use of communication infrastructure, electronic networks, and malign cyber activities targeting U.S. persons, institutions, social media platforms, and other businesses. However, the Department **still lacks a counter foreign interference strategy to guide all Departmental activities**. **The Department should** establish a lead coordination mechanism with clearly defined roles and responsibilities supported by Departmental leadership.

DHS should formally establish an inter-agency task force that would include all federal entities involved in countering the threat of FI, such as, Department of Justice, Federal Bureau of Investigations, State Department, Department of Defense, Treasury, National Security Council, and the Federal Communications Commission. **DHS should also ensure that all approved strategies and policies for countering foreign influence are appropriately resourced and funded**.

Finally, it is critical to develop a whole-of-society approach where government agencies have a meaningful liaison with the private sector, media, technology companies, academia, think tanks, and the general public. **DHS can play a leading role in raising public awareness efforts, ensuring effective coordination, and providing information sharing mechanisms to identify and help counteract foreign influence operations.**

INTRODUCTION

The terms "foreign influence" and "foreign interference" have become synonymous with efforts by Russia to impact both public sentiment as well as elections in the United States, points that have been reinforced following the publication of the "Special Counsel Investigation into Russian Interference in the 2016 Presidential Election" report.

While efforts by Russia provide compelling examples of "foreign influence" and "foreign interference," they do not represent the entire landscape of attempted foreign influence – either by Russia or others – in elections or other events, whether in the United States or across any number of democracies, particularly in Europe. Indeed, numerous countries have been alleged to be involved in attempts at "foreign influence" and "foreign interference," to include China[1], North Korea, Iran and various other Middle Eastern states.[2]

Foreign Interference/Influence (FI) is defined as: "Malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."

A particular form of FI, Information Activities (IA) is defined as: "Activities undertaken to shape public opinion or undermine trust in the authenticity of information. Use of new and traditional media to amplify divides and foment unrest in the homeland, sometimes coordinated with illicit cyber activities."

Foreign state actors engaged in "foreign influence" and "foreign interference" often target public institutions, private sector entities as well as individuals. They seek to influence U.S. policy and elections, disrupt markets, seed conflict, and sow societal discord to undermine our democracy.

Moreover, malign foreign influence efforts may come not only from state actors, but from individuals as well as organizations who are motivated by criminal intent and/or ideological objectives.

The United States can be especially vulnerable to foreign influence due to a number of factors, to include: its nature as a democracy that values, promotes and protects freedoms of speech and expression; an increasing reliance on platforms such as social media that, by their nature, allow for increasingly siloed verticals of information sharing and receptivity, as well as; the American population's decreasing trust in various institutions, to include government and traditional news media sources.[3]

---

[1] For more information on Chinese foreign influence campaigns, please see: Williams, Rush Doshi and Robert D. "Is China Interfering in American Politics?" *Brookings*, October 2, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/; "China's Global Information and Influence Campaign." *Council on Foreign Relations*. https://www.cfr.org/project/chinas-global-information-and-influence-campaign; Grace, Abigail. "China's Influence Operations Are Pinpointing America's Weaknesses." *Foreign Policy.* https://foreignpolicy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses/.

[2] Axelrod, Tal. "FBI Chief: Foreign Influence Campaigns Continually Targeting US." *The Hill*, March 5, 2019. https://thehill.com/policy/national-security/432776-fbi-chief-foreign-influence-campaigns-continually-targeting-us.

[3] West, Darrell M. "How to Combat Fake News and Disinformation." *Brookings*, December 18, 2017.

Given the above, when foreign influence and interference manifests itself through the active effort of spreading disinformation, the consequences can be dire; the use of disinformation must be viewed as a revolutionary tool of warfare, which does not require direct acts of violence but has significant potential to disrupt society, business, and politics. At the same time, and adding to the complexity and virulence of the issue, disinformation efforts can be relatively inexpensive to mount and difficult to counter efficiently without significant coordination and cooperation.[4]

The Disinformation Model has a singular goal of disruption and four key stages to deliver on this goal:

1. **Digital Message Creation** - across video, audio, image, and text formats.
2. **Distribution & Dissemination** - across traditional and social media as well as by individuals and organizations.
3. **Destination Environment and Audiences** to both the Supporters (Receptive); the Opens (Neutral) and the Sceptics (Rejector)
4. **Development or Decline** – whether the message spreads and its idea grows or withers.

At the same time, disinformation campaigns can be utilized to not only target the United States, but also to indirectly target her allies with the goal of sowing mistrust within or between democratic countries, and in democratic institutions.[5]

In all of this, the freedoms established by our democratic system to protect free and open debate and the very institutions, systems and applications that support that right to debate, are being exploited by foreign adversaries to undermine the unity and power of the United States.

Given the potential impact of the above efforts, the subcommittee believes that the last official U.S. government statement addressing the threat of foreign influence campaigns[6] was too limited, concentrating on altering votes and not addressing disinformation campaigns or attempted election interference in the broader sense.

Adding to the complexity of this issue, since foreign actors seeking to destabilize the U.S. may have differing goals[7], it is essential to understand each actor's objective and their methods in order to devise effective strategies to counter their influence attempts.

---

https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

[4] "…The historian Timothy Snyder observed that Russia's annual budget for cyberwarfare is less than the price of a single American F-35 jet." (https://www.theatlantic.com/ideas/archive/2018/07/the-great-russian-disinformation-campaign/564032/)

[5] Bayer et al. "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States," Policy Department for Citizens' Rights and Constitutional Affairs, The European Parliament. http://aei.pitt.edu/97042/1/disinformation_and_propaganda.pdf.

[6] "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," October 19, 2018. https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections.

[7] Kendall-Taylor, Andrea, and David Shullman. "How Russia and China Undermine Democracy," *Foreign Affairs*, October 2, 2018. https://www.foreignaffairs.com/articles/china/2018-10-02/how-russia-and-china-undermine-democracy.

Although legislation can be an important component of countering foreign influence – such as the Countering Foreign Propaganda and Disinformation Act 2016[8] – no legislation can keep pace with current technological advances, which appear to be increasing the speed and sophistication by which foreign influence campaigns can be devised and executed.

Current and rapidly evolving technologies make it possible to revitalize Cold War 'active measures' that were once used to advance the cause of communism. Once considered punitively expensive and extremely time-consuming for a very limited return, these tactics – which include propaganda and influence efforts – have now been streamlined by technology, facilitating rapid, remote manipulation and low cost targeting simply using a smart phone and a social media account.

Foreign influence and disinformation should be seen as a continuous, ongoing assault on the United States, rather than a series of discrete, targeted, event-specific campaigns.[9] Foreign influence toolkits should be received in the same way as "Advanced Persistent Threats" are in the world of cybercrime – once a target, always a target. The exploit is simply modified or evolves where new technology permits, to make it more effective next time and will include:

False Information Operations – deliberately using false narrative through traditional media and social media outlets to manipulate and mislead the population and the weaponization of information to undermine organizations, democratic processes, or to polarize divisions.

Deep Fake Technology (DFT) – the expansion and evolution of Artificial Intelligence (AI) that makes it literally possible to "put word into someone's mouth" or alter images and/or video with the ongoing argument being not necessarily what was said or seen but whether the party seen to make the comment or appear at a location was actually real.

A Deep Fake is an AI-assisted video created by taking a number (usually hundreds or thousands) of photos of a source person. The source of a Deep Fake is a series of still photographs, pieced together so that the result of a Deep Fake is a video with a replaced face.

Deep Video Portrait (DVP) – Deep Fake technology and DVP are similar, but different techniques, with DVP being used in Hollywood movies and even YouTube videos.

DVP has two important differences from DFT: (1) it does not replace the face, only manipulates the features and; (2) the source for a DVP originates from a live-action actor, not from individual photographs.

DVP is not face swapping. It is facial manipulation. This means that DVP creators can do things like make the target blink, open the mouth, raise the eyebrows, and turn the head side to side based on the source actor's movements. As a result, DVP tends to be more believable than DFT.

[8] Kinzinger, Adam. "H.R.5181 - 114th Congress (2015-2016): Countering Foreign Propaganda and Disinformation Act of 2016." May 10, 2016. https://www.congress.gov/bill/114th-congress/house-bill/5181/all-info.
[9] Fly, Jamie M., and Laura Rosenberger. "The Mueller Report Shows Politicians Must Unite to Fight Election Interference," *Foreign Affairs*, April 22, 2019. https://www.foreignaffairs.com/articles/2019-04-22/mueller-report-shows-politicians-must-unite-fight-election-interference.

The United States currently has no law specifically dealing with Deep Fakes. Often any debate or investigation is unable to redress the balance when unsuspecting members of the public have already watched the video and are "locked in" to already believing that it actually took place.

Cyberwarfare – exploiting attacks on the critical infrastructure and digital infrastructure to either shutdown or support other forms of attack or other parts of a subversive operation. Whilst existing technology lends itself to attacking electronic and digital election systems, this is not the limit of its capabilities in this area.

Another example might be intentionally launching a distributed denial of service attack with a botnet against a news media organization expected to adversely report on other malign operations carried out by the foreign influencer.

Financial Influence – transferring money into another country intending to use it to obtain political leverage and fund other operations such as corruption schemes intended to recruit proxies to support media campaigns, from within in the same way as cold war espionage operations.

Backing Extreme Political Groups – providing financial and logistical support for extreme political and advocacy groups designed to promote a more friendly agenda towards the foreign government supplying the support or to support extremist and divisive views inside the U.S. In many cases, these groups may not even know the true source of donations or other support as they are skillfully engineered into a belief that makes their acceptance more palatable.

Currently it appears that there is no single or joint body in the U.S. government in charge of coordinating efforts to counter foreign influence campaigns, such as countering disinformation, combatting the CFI cyber threat, or investigating support for extreme political groups. These tasks may be carried out by numerous federal organizations as part of other mandates or other duties.

Even when issues are identified they are often dealt with in the same way as fire-fighting: reactively, dealing with the incident rather than proactively introducing greater safeguards and preventative measures.

Often the source of sustained disinformation campaigns targeting the public are not addressed due to a lack of leadership and coordination. Simply, no one seems to know who would be responsible for countering that particular threat. For the same reason, it is difficult to assess the true scale of the issue because, again, no one has taken direct ownership of the problem.

On September 18, 2018 Secretary Nielsen instructed that the Homeland Security Advisory Council establish a new subcommittee titled the "Countering Foreign Influence Subcommittee" to provide recommendations regarding the following issues surrounding foreign influence campaigns:

1) Provide an assessment of all DHS entities that currently have equities in countering foreign influence.

2) Identify additional DHS entities at the Headquarters and Component levels that have perceived capabilities to counter foreign influence threats.

3) Identify the current nation states and illicit groups involved in foreign influence campaigns and provide a forward-looking assessment of their perceived capabilities in conducting future influence campaigns. This assessment should include recommendations on how DHS can best prepare for perceived future foreign influence campaigns.

4) Provide an assessment of private sector entities and infrastructure that are targeted by foreign influence campaigns and identify support mechanisms and oversight capabilities that DHS has to assist these entities.

This interim report by the Countering Foreign Influence Subcommittee attempts to provide recommendations related to the four specific tasks mandated by the Secretary and other closely related topics.

This page is intentionally left blank.

RECOMMENDATIONS OF THE INTERIM REPORT

Tasking 1

1. DHS should establish a countering foreign interference strategy and policy to guide all Departmental activities.

2. DHS should establish a lead coordination mechanism/organization with clearly defined roles and responsibilities supported by Departmental leadership.

3. DHS should recommend and support the creation of an interagency organization similar to the NCTC co-lead by DHS and FBI.

4. DHS to build a robust response team to immediately address and correct deficiencies and maintain effort permanently, not just during election cycles.

5. DHS should ensure that all approved strategies and policies for countering foreign influence are appropriately resourced.

6. DHS should ensure that all DHS related entities are adequately funded and staffed for this mission.

7. DHS should ensure that all staff are adequately trained for the mission.

8. DHS should attract an effective and appropriate number of employees for its mission, including private sector consultants with technical and operational capabilities related to foreign influence matters.

9. DHS should develop options that aim to retain a stable workforce in this highly competitive and rapidly changing workspace.

10. DHS to establish effective interagency collaboration regarding potential and actual foreign threats.

11. DHS to arrange the provision of adequate authorities, resources, funding and staffing for the Office of Intelligence and Analysis (I&A) for the monitoring, analysis and collecting on all threats related to countering foreign influence.

Tasking 2

1. Establish effective protocols for CISA and other DHS entities to interact with State Fusion Centers and other federal agencies involved in these matters.

2. Identify areas to strengthen CISA authorities so as to effectively meet the Department's needs.

3. Adequately prioritize funds through the current DHS grant programs and U.S. government coordination – to help protect state and local entities contend with the

potential for foreign influence in the 2020 election cycle and beyond.

4. DHS to continuously work with state and local entities to enhance and strengthen cyber security for the electoral infrastructure in order to diminish and prevent the capabilities of malign foreign actors to interfere in our democracy and diminish confidence in the voting system.

5. Align DHS efforts to help counteract foreign influence with DHS's work in support of the 16 critical infrastructure sectors by effectively focusing on critical infrastructure assets, systems and networks, both physical and virtual.

Tasking 3

1. DHS should work with Congress to develop clear authorities for the Department in the CFI mission space.

2. DHS should identify and establish departmental intelligence and analysis requirements.

3. DHS should introduce standardized procedures to better serve the reporting of foreign influence incidents.

Tasking 4

1. DHS to play a leading role in working with other entities to raise public awareness efforts, ensure effective coordination and information sharing mechanism to identify and help counteract foreign influence operations.

2. DHS to ensure adequate and effective coordination with key social media firms.

3. DHS to develop better information sharing among DHS related agencies, social media firms, technology companies and the general public to identify and help counteract foreign influence operations.

4. DHS to seek legislation that provides adequate protection for DHS entities, social media platforms, and cyber security companies to share information on online propaganda.

5. DHS to support building confidence in the system by transparency, publicly acknowledging cyber-attacks, announcing actions taken and advising the general public of attacks and corrective and preventative actions.

TASKING 1

Provide an assessment of all DHS entities that currently have equities in countering foreign influence.

The Challenge

It is clear that while some federal agencies think they are leading the work to counter foreign influence, no one entity has officially been provided with a mandate to do so. While it is recognized that no one single agency can be solely responsible for the issue, coordination and leadership is required. DHS should have a leading role but, more broadly, an inter-agency task force is required that would include those entities which have authorities and capabilities to impact this issue, to include in addition to DHS: Department of Justice, State Department, Department of Defense, Treasury, National Security Council, and the Federal Communications Commission.

Foreign influence activities are a direct threat to the national security of the United States, and seeks to undermine our very democracy. It is critical that all components of the government, as well as different sectors within our society, work together to counter this threat.

Inside the DHS, almost all operating components have a role to play in countering malign foreign influence that entails the use of electronic networks, electronic media, and targeted at U.S. persons, institutions, social media platforms and other businesses.

In addition to DHS, certain other U.S. government agencies have essential roles in defensive work associated with foreign influence (especially FBI and U.S. intelligence community assets).

For example, the U.S. Cyber Command reportedly assisted in successfully disrupting and deterring attempts of foreign influence targeting the midterm elections in October 2018.[10] This was accomplished through a range of tactics, including: gaining access to foreign networks; reaching out directly to individuals working for the Internet Research Agency to warn them about interfering in U.S. elections; temporarily disrupting the networks, preventing adversaries from deploying disinformation to create widespread discord among Americans during election season.[11] The operation, codenamed 'Synthetic Theology,' was a large-scale effort that involved the National Security Agency (NSA) along with other government agencies.

Initial Findings

- Numerous U.S. government entities are key participants in managing the risks associated with foreign influence efforts. These include DHS, FBI, various intelligence agencies, the National Security Council, the military, and others.

[10] Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *The Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[11] *Ibid.*

- The DHS Secretary ultimately "owns" the Department's mission plan and execution for DHS obligations regarding foreign influence concerning U.S. elections. The Secretary has to be adequately supported internally to be successful in DHS's mandate to help reduce the risk of malign foreign influence in near-term elections and beyond.

- DHS' Cybersecurity and Infrastructure Security Agency (CISA) has all the components necessary to take a leading part in the countering of foreign influence, disinformation, and election related cyber-attacks (discussed in greater detail below).

- Virtually almost all entities at DHS take part in countering foreign influence. For example, through the cyber security unit of Homeland Security Investigations, the capability and capacity to counter the threat of disinformation exists and the unit is able to assist, but apparently it has not yet been tasked or resourced to do so.

- Most research emphasizes a multidisciplinary approach to countering foreign influence, which includes government, legislation, technological advances, private companies assuming their responsibility, education, and civil society engagement.

- By virtue of Section 3 of the Countering Foreign Propaganda and Disinformation Act of 2016, the State Department was to establish a Center for Information Analysis and Response to:

    1. Lead and coordinate the collection and analysis of information on foreign government information warfare efforts;

    2. Establish a framework for the integration of critical data and analysis on foreign propaganda and disinformation efforts into the development of national strategy; and

    3. Develop and synchronize government initiatives to expose and expose foreign information operations directed against U.S. allies and interests.

Recommendations

1. DHS should establish a countering foreign interference strategy and policy to guide all Departmental activities.

2. DHS should establish a lead coordination mechanism/organization with clearly defined roles and responsibilities supported by Departmental leadership.

3. DHS should recommend and support the creation of an interagency organization similar to the NCTC co-lead by DHS and FBI.

4. DHS to build a robust response team to immediately address and correct deficiencies and maintain effort permanently, not just during election cycles.

5. DHS should ensure that all approved strategies and policies for countering foreign influence are appropriately resourced.

6. DHS should ensure that all DHS related entities are adequately funded and staffed for this mission.

7. DHS should ensure that all staff are adequately trained for the mission.

8. DHS should attract an effective and appropriate number of employees for its mission, including private sector consultants with technical and operational capabilities related to foreign influence matters.

9. DHS should develop options that aim to retain a stable workforce in this highly competitive and rapidly changing workspace.

10. DHS to establish effective interagency collaboration regarding potential and actual foreign threats.

11. DHS to arrange the provision of adequate authorities, resources, funding and staffing for the Office of Intelligence and Analysis (I&A) for the monitoring, analysis and collecting on all threats related to countering foreign influence.

This page is intentionally left blank.

TASKING 2

Identify additional DHS entities at the Headquarters and Component levels that have perceived capabilities to counter foreign influence threats.

The Challenge

The Department of Homeland Security has a broad range of authorities and capabilities that could be leveraged to combat foreign influence operations. To date, these authorities and capabilities have not been fully leveraged. Any DHS strategy to combat disinformation should ensure all DHS authorities and capabilities are integrated into the Department's approach.

In particular, DHS' Cybersecurity and Infrastructure Security Agency (CISA) has all the components necessary to take a leading part in countering foreign influence, disinformation and election related cyber-attacks. CISA's mission includes a focus on countering:

1. Malign foreign influence targeted against U.S. persons, public institutions (federal, state and local), and U.S. businesses.
2. Cyber malign activities (not including influence operations) that are operated by actors based in the U.S.

To better perform its mission, CISA needs very close coordination with other DHS operating components; it has embedded personnel in certain DHS components and, to date, has welcomed reciprocal assignments from within relevant DHS components.

CISA's strength is in speaking to and supporting the American public regarding cybersecurity related risk. To counter election manipulation by foreign actors, numerous U.S. government agencies must work to support state and local officials; DHS has a unique role to help educate the American public about these threats.

Other components within DHS also have the potential to play an important role in countering the threat of foreign influence activities, such as the Office for Intelligence and Analysis (I&A), Homeland Security Investigations (HIS) Cyber Crimes Center (C3), and the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC).

Initial Findings

- Greater intelligence sharing is essential between all major parties and mechanisms needs to be in place to ensure that all levels of government, including local election officials, are aware of potential threats.

- While it is clear that foreign influence campaigns are not limited to elections, there would appear to be increased use at these times and it is unclear where or if the mechanics of foreign influence and disinformation fits with the definition of "Election Security." Even if such a definition is encompassing, it is questionable as to whether local election

officials either have the know-how or the resources to focus on this threat.

- The lack of resources at the local level during elections is a real concern with a lack of training, cyber expertise, and even sufficient personnel, together with borderline obsolete systems providing fertile ground for exploitation by foreign actors.

- There is a lack of understanding, particularly in local election officials and the voting population, so that even if some interference was suspected, it is unlikely that they would know what mitigation or response action to take.

- The intense DHS interactions with state and local officials and social media staff in 2018 were successful and offered valuable lessons learned for the next election cycle.

Recommendations

1. Establish effective protocols for CISA and other DHS entities to interact with State Fusion Centers and other federal agencies involved in these matters.

2. Identify areas to strengthen CISA legislation so as to effectively meet the Department's needs.

3. Adequately prioritize funds through the current DHS grant programs and U.S. government coordination – to help protect state and local entities contend with the potential for foreign influence in the 2020 election cycle and beyond.

4. DHS to continuously work with state and local entities to enhance and strengthen cyber security for the electoral infrastructure in order to diminish and prevent the capabilities of malign foreign entities to interfere in our democratic system and diminish confidence in the voting system.

5. Align DHS efforts to help counteract foreign influence with DHS's work in support of the 16 critical infrastructure sectors by effectively focusing on critical infrastructure assets, systems and networks, both physical and virtual.

This page is intentionally left blank.

TASKING 3

Identify the current nation states and illicit groups involved in foreign influence campaigns and provide a forward-looking assessment of their perceived capabilities in conducting future influence campaigns. This assessment should include recommendations on how DHS can best prepare for perceived future foreign influence campaigns.

The Challenge

Disinformation campaigns have been and are used as a tool by state and non-state actors alike.

Historically, a number of states have devised disinformation campaigns to police and influence their own population e.g. Russia, North Korea, Turkey and the Philippines.[12]

Russia, China, Iran, and Saudi Arabia are examples of states that have used disinformation as a foreign policy tool against adversaries, also known as foreign influence.

It must be noted that no two state actors have exactly the same objectives when they devise disinformation campaigns. For example, the known Chinese disinformation campaigns in the United States have focused on pro-Chinese propaganda and strategic economic policy[13], whereas known Russian campaigns focused on political discourse and election infrastructure.[14]

On the other hand, non-state actors, such as the so-called Islamic State are believed to have used disinformation campaigns in order to target and infiltrate domestic movements in the United States.[15]

In particular, there are examples of Russian foreign interference and disinformation campaigns being used against the United States and her allies:

- Russia originally denied it had a military presence in Crimea and Eastern Ukraine but then gave their invasion legitimacy by inventing stories including the crucifixion of a Russian child by Ukrainian neo-Nazis and blamed Ukrainians for shooting down a Malaysian civilian airliner (MH17) using a Russian BUK ground-to-air missile.[16]

The Russian effort has involved overt activities by government agencies, state-backed

[12] "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," October 27, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017.
[13] "China's Global Information and Influence Campaign." *Council on Foreign Relations*. https://www.cfr.org/project/chinas-global-information-and-influence-campaign.
[14] Polyakova, Alina. "What Do Russian Disinformation Campaigns Look like, and How Can We Protect Our Elections?" *Brookings*, October 3, 2018. https://www.brookings.edu/blog/brookings-now/2018/10/03/what-do-russian-disinformation-campaigns-look-like-and-how-can-we-protect-our-elections/.
[15] See for example: Wilson, Darren. "Situation Report." Ferguson, Missouri: Federal Bureau of Investigation, August 20, 2014. https://ccrjustice.org/sites/default/files/attach/2018/03/FBI%20881.pdf;
[16] "Alternative Reality." *The Economist*, May 30, 2015. https://www.economist.com/europe/2015/05/30/alternative-reality.

media and paid Internet trolls, as well as covert operations, including cyber activities by believed intelligence agents.

Social media in particular has been one of the main targets of the disinformation campaign:

- The Internet Research Agency (IRA) based in St. Petersburg, Russia reportedly hired hundreds of 'trolls' to open social media accounts and post false news stories and socially divisive content across a range of platforms.[17]

- IRA has been identified as an entity with links to the Kremlin.[18]

- Facebook reported that the IRA posted content reached more than 140 million of its users.

According to the Alliance for Securing Democracy[19], Russian-linked accounts largely comment on three categories:

- Social and political topics of interest to American audiences

- Geopolitical topics of interest to the Kremlin

- Apolitical topics used to attract and engage followers

On American issues, Russian-linked accounts do not need to be persuasive, as they target audiences with messages tailored to their preferences, so that the content shared merely solidifies preconceived beliefs.

The September 2018 criminal complaint against Elena Khusyaynova, the IRA accountant accused of conspiracy to defraud the United States, includes these words:

> *" ... members of the Conspiracy used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment, the Confederate flag, race relations, LGBT issues, the Women's March and the NFL anthem debate. Members of the Conspiracy took advantage of specific events in the United States to anchor their themes, including the shootings of church members in Charleston, South Carolina, and the concert attendees in Las Vegas, Nevada; the Charlottesville "Unite the Right" rally and the associated violence; police shootings of African- American men; as well as the personnel and policy decisions of the current U.S. administration."*[20]

The conclusion of these debates is irrelevant to the Kremlin, who simply seek to amplify

[17] Chen, Adrian. "The Agency." *The New York Times*, June 2, 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.
[18] Ibid.
[19] Schafer, Bret. "A View from the Digital Trenches – Lessons from Year One of Hamilton 68." *Alliance for Securing Democracy*, November 19, 2018. http://www.gmfus.org/publications/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68.
[20] United States of America v. Elena Alekseevna Khusyaynova (Eastern District of Virginia September 28, 2018).

extreme views of existing divisive issues, to poison public discourse and thereby endear themselves to "like-minded" users, who in turn may freely accept other disinformation without challenge.[21]

In June 2017, DHS officials reported that individuals linked to the Kremlin attempted to infiltrate election-related computer systems in more than 20 U.S. states. Authorities to date believe that whilst the Russian hackers did not tamper with the vote count, they were probing election systems for vulnerabilities.

Initial Findings

- Sustained disinformation campaigns targeting the public are not addressed because there is still a lack of awareness as who would be responsible for countering the threat.

- During and between elections, foreign actors have been active on social media spreading inaccurate information.

- A lack of confidence in the voting system undermines the process and voter confidence in elections.

- In the lead up to the 2018 midterm elections, a prevention campaign involving Voatz, the mobile election platform for servicemen and women overseas, succeeded when they first put out insecure equipment and gathered information about the types of attack and tactics used against it. This information was fed back as prevention systems to protect the systems and no attacks are known to have taken place.

- Disinformation campaigns have evolved from blunt audience engagement in 2016, to more tailored, sophisticated and focused disinformation e.g. targeting highly-engaged community of interest. This tactic can again be seen (using the cyber analogy), as the evolution from Spam Phishing attacks – High Volume – Low Sophistication – Random Uptake to Spear-phishing attacks – Low Volume – Well Researched – High Uptake.

- Foreign influence attempts using social and cultural organizations to recruit white nationalists and other susceptible demographics to attend training camps that promote pro-Russian ideology, which is therefore anti-United States and anti-European Union.

- This is not just an American issue and therefore we need to build on existing mechanisms for government coordination with our allies; e.g. Canada, Australia and European Union countries whilst also learning lessons from their experiences and coordinate efforts.

Recommendations

1. DHS should work with Congress to develop clear authorities for the Department in the CFI mission space.

[21] Schafer, Bret. "A View from the Digital Trenches – Lessons from Year One of Hamilton 68." *Alliance for Securing Democracy*, November 19, 2018. http://www.gmfus.org/publications/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68.

2. DHS should identify and establish departmental intelligence and analysis requirements.
3. DHS should introduce standardized procedures to better serve the reporting of incidents.

This page is intentionally left blank.

TASKING 4

Provide an assessment of private sector entities and infrastructure that are targeted by foreign influence campaigns and identify support mechanisms and oversight capabilities that DHS has to assist these entities.

The Challenge

Close and meaningful liaison with corporate organizations is an enormous task for any government because the needs of both parties are not necessarily a natural or convenient fit.

Ideally, the social media companies and the press will be more vigilant about the integrity of reports and checking that account holders and sources are real, whereas the imperative for social media companies, in particular, is fast public information sharing with minimal oversight.

In attempting to bridge this gap, partnerships have been developed with the major social media platforms.

- At the recent Paris Summit (dubbed "The Christchurch Call") on May 15, 2019 a digital consortia of Alphabet (Google), Facebook, and Twitter committed to develop and use rules, algorithms and direct intervention to curb uploading, promotion, amplification, and distribution of violent extremist content on their platforms. There were few previous commitments in the past, but progress has been always slow.

- Facebook is facing continuous challenges but has created a number of mechanisms to deal with electoral integrity. They have the apparatus in place that allows them to engage and communicate internally to deal in the event of a crisis.

- Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants and that 170 Instagram accounts had posted approximately 120,000 pieces of content.

- In November 2017, a Facebook employee testified that Facebook had identified 470 IRA-controlled accounts that had collectively made over 80,000 posts over two and a half years to August 2017.[22] Facebook estimate that IRA reached as many as 29 million individuals through their Facebook accounts, and this exposed 126 million persons after sharing.

- Twitter is a smaller platform but due to its design still carries a larger portion of the blame for disinformation sharing; its product is information and it is easy to understand how to use it for disinformation campaigns. Research is a simpler task than some other platforms and therefore this gives the impression that their data is more accessible.

[22] RUSSIA INVESTIGATIVE TASK FORCE HEARING WITH SOCIAL MEDIA COMPANIES, § Permanent Select Committee on Intelligence (2017). https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Transcript-20171101.pdf.

- In 2018, Twitter identified and released information from 3,814 IRA-linked Twitter accounts and stated that they believed that approximately 1.4 million people had been in contact with an IRA-controlled account.[23] These accounts had posted nearly 176,000 tweets in the ten weeks prior to the 2016 presidential elections.

- Google and YouTube currently lack a robust policy team like other platforms. Their company is in the process of restructuring and they also have new leadership, which could give them the advantage of reacting faster to lessons learned as they do not have existing rigid practices to change.

- DHS can work with advertisement agencies and media entities, both traditional and social, on developing business models that disincentivizes misinformation and falsehood.

During the 2018 elections, information sharing took place between Facebook and law enforcement, following the allegations about the IRA, the Russian troll factory. The government connected Facebook and targeted journalists with the research community to debunk the falsehood promoted by the IRA. Journalists are important to efforts for countering foreign disinformation and should understand they are both a conveyor of information to the American public, as well as, a target of foreign influence activities. Appropriate information sharing can assist both companies and journalists to address the risks of foreign influence.

Working with and understanding other technologies, such as point to point information sharing platforms, for instance, Telegram and WhatsApp discloses other issues. For example, encryption is another challenge and greater ties with these operators need to be explored. One route would be possibly offering assistance with recent hacking allegations against WhatsApp users.

Initial Findings

- The information sharing protocols between the intelligence community, state and local officials, the public and, most importantly, media and social media companies is inconsistent and therefore insufficient processes are in place to ensure that necessary information is shared.

- Efforts to raise awareness of the issue of foreign influence need to be approached in a bi-partisan non-political – "all our liberties are at risk" way.

- Policy makers and private companies, for instance in Silicon Valley, are now in danger of settling for a sentiment of compliance as no extreme events took place during the 2018 elections. This would be a mistake as we have to anticipate renewed efforts in the lead up to 2020 and beyond.

Recommendations

1. DHS to play a leading role in working with other entities to raise public awareness efforts, ensure effective coordination, and provide information sharing mechanisms to

[23] "Update on Twitter's Review of the 2016 US Election." January 19, 2018. https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.

identify and help counteract foreign influence operations.

2. DHS to ensure adequate and effective coordination with key social media firms.

3. DHS to develop better information sharing among DHS related agencies, social media firms, technology companies and the general public to identify and help counteract foreign influence operations.

4. DHS to seek legislation that provides adequate protection for DHS entities, social media platforms, and cyber security companies to share information on online propaganda.

5. DHS to support building confidence in the system by transparency, publicly acknowledging cyber-attacks, announcing actions taken and advising the general public of attacks and corrective and preventative actions.

This page is intentionally left blank.

APPENDIX A – PANEL MEMBER BIOGRAPHIES

Ali H. Soufan (Chair)

Ali H. Soufan is the Chairman and CEO of The Soufan Group, LLC, and has been a member of the Homeland Security Advisory Council since September 2012. Mr. Soufan is a former FBI Supervisory Special Agent who investigated and supervised highly sensitive and complex international terrorism cases, including the East Africa Embassy Bombings, the attack on the USS Cole, and the events surrounding the 9/11 attacks. Mr. Soufan also served on the Joint Terrorist Task Force, FBI New York Office, where he coordinated both domestic and international counterterrorism operations. He has received numerous awards for his counter-terrorism work, including the FBI Director's Award for Excellence in Investigation and the Respect for Law Enforcement Award. Mr. Soufan is the author of The New York Times Top 10 Bestseller, "The Black Banners: The Inside Story of 9/11 and the War Against al-Qaeda" and a recipient of the Ridenhour Book Prize.

Michael P. Jackson (Vice Chair)

Michael P. Jackson is the President and Founder of Firebreak Partners a company that provides specialized security and technology consulting services for critical infrastructure assets. On March 10, 2005, the U.S. Senate confirmed Mr. Jackson to serve as Deputy Secretary of the U.S. Department of Homeland Security (DHS). Mr. Jackson served as DHS' chief operating officer, with the responsibility to manage the Department's day-to-day operations. Previously, Mr. Jackson served as Senior Vice President of AECOM Technology Corporation, where he was responsible for AECOM government relations globally and served as Chief Operating Officer of AECOM's Government Services Group. Mr. Jackson also served as Deputy Secretary of the U.S. Department of Transportation (DOT) from May 2001 to August 2003. As DOT, Mr. Jackson was responsible for day-to-day operations of an organization that grew to a $68 billion annual budget supporting over 179,000 employees following the terrorist attacks of 9/11/01. In 2004, Mr. Jackson was appointed to serve on the President's Commission on Implementation of United States Space Exploration Policy, which provided management recommendations to the President on NASA and its future mission management. Mr. Jackson also held positions under President George H. W. Bush's administration, as Special Assistant to the President for Cabinet Liaison and later as Chief of Staff to the Secretary of Transportation. He held several positions reporting to the Secretary of Education under President Ronald Reagan's administration. He was a researcher at the American Enterprise Institute and taught political science at the University of Georgia and at Georgetown University. Mr. Jackson graduated from the University of Houston with a B.A. and received a Ph.D. with distinction from the Government Department at Georgetown University in 1985.

John R. Allen

John R. Allen is a retired four-star U.S. Marine General who served as the Commander of the NATO International Security Assistance Force and the Commander of U.S. Forces Afghanistan from 2011 to 2013, the pivotal point in the war. General Allen recently served as Special Presidential Envoy for the Global Coalition to Counter ISIL. He is the first Marine in history to command a theater of war, and is the longest serving commander in that conflict. Concluding a distinguished 38 year career in the spring of 2013, General Allen served as Senior Advisor to both the Secretaries of Defense and State on Middle East Security, and has associations with the

Brookings Institution, the Johns Hopkins School of Advanced International Studies, the Atlantic Council, and Council on Foreign Relations. He holds numerous U.S. personal and international decorations, among them the: Defense Distinguished Service Medal, the Defense Superior Service Medal, the Legion of Merit, The Leftwich Leadership Trophy, the Global War on Terrorism Service Medal, the Humanitarian Service Medal, the NATO Meritorious Service Medal, the Afghan Ghazi Mir Bacha Khan Medal, the French Legion d'Honneur, the Commander's Cross of the Order of Merit of the Polish Republic, the Taiwan Order of the Resplendent Banner with Special Cravat, and the Mongolian Meritorious Service Medal, First Class.

Paul Goldenberg

Paul Goldenberg is the President and CEO of Cardinal Point Strategies (CPS), LLC, a strategic advisory and business intelligence consulting firm. Mr. Goldenberg served as founder and first National Director of the Secure Community Network, the nation's first faith-based information sharing analysis center recognized by DHS as a national model. Mr. Goldenberg is an internationally recognized transnational security expert providing the U.S. government and private sector strategic counseling and governance on a full array of national security related issues at the nexus of terrorism, technology, national security, law enforcement, community engagement and policing. Mr. Goldenberg's public career includes more than two decades as the first State Chief of the Office of Bias Crimes and Community Relations in New Jersey leading the nation's first full time State Attorney General's effort focusing on hate crimes, domestic terrorism, targeted violence, and community engagement, Director of the nation's 6th largest county social service and juvenile justice system, and as a law enforcement official leading investigation efforts for cases in domestic terrorism, political corruption, and organized crime. Mr. Goldenberg played a key role in setting policy for the legislation and investigation of ethnic terrorism and hate crimes in roles such as senior law enforcement advisor to the Organization for Security and Cooperation in Europe, US department of Justice, DHS, and for numerous Canadian police and security agencies. He is a senior fellow with the Rutgers University Miller Center for Community Protection and Resilience.

John Magaw

John Magaw is a domestic and international security consultant who most recently served as the Under Secretary for Security at the Department of Transportation in 2002. In that role, Mr. Magaw was responsible for the implementation of the Aviation and Transportation Security Act of 2001. Mr. Magaw also previously served as the Acting Director of the Federal Emergency Management Agency (FEMA) and led the Office of National Preparedness with FEMA. Magaw has also served as the Director of the Bureau of Alcohol, Tobacco, and Firearms from 1993 to 1999 and as the Director of the Secret Service from 1992 to 1993.

Paul Stockton

Dr. Paul Stockton is the Managing Director of Sonecon LLC, and an internationally-recognized leader in infrastructure resilience, continuity planning, installation and personnel security, and U.S. national security and foreign policy. From June 2009 until January 2013, Dr. Stockton was Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs at the U.S. Department of Defense, where he served as the Department's Domestic Crisis Manager. In this position he assisted in leading the response to Superstorm Sandy, Deepwater Horizon, and other disasters. Dr. Stockton was also responsible for Departmental programs strengthening security

cooperation with partner nations in the Western Hemisphere, leading talks on Defense Cooperation Agreements with Peru, Brazil, and other key countries, as well as defense policy coordination with Mexico and Canada. In September 2014, Secretary Hagel named Stockton the co-chair of the Independent Review of the Washington Navy Yard Shootings, which recommended major changes to the Department of Defense's security clearance system. He was twice awarded the Department of Defense Medal for Distinguished Public Service, the Pentagon's highest civilian honor, and a Distinguished Public Service Medal from the Department of Homeland Security.

Chad Sweet

Chad Sweet is the Co-Founder & CEO of the The Chertoff Group, a global advisory firm and investment bank exclusively focused on the security sector. Mr. Sweet advises companies and governments on their security and on mergers and acquisitions (M&A) in the security industry. With over a decade of investment banking experience, Mr. Sweet has been involved in more than $5 billion of successful M&A and capital formation engagements. Mr. Sweet was the former Chief of Staff of DHS and served in the CIA. He currently serves as Chairman of Trustwave Government Services as well as a Director of the corporate boards of Coalfire and Salient CRGT. Finally, in the non-profit sector, he is a Senior Fellow at the George Washington Homeland Security Policy Institute, a Director on RAND's Global Center for Risk & Security, a Director of the Board of the Economic Club of Washington and a frequent commentator on security issues for FOX, CNN, CNBC and Bloomberg TV.

APPENDIX B – TASK STATEMENT

Secretary
U . S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: Judge William Webster
Chair, Homeland Security Advisory Council

FROM: Kirstjen M. Nielsen
Secretary

SUBJECT: **Countering Foreign Influence Subcommittee**

Pursuant to the September 18th, 2018 HSAC meeting, I instruct the Homeland Security Advisory Council (HSAC) to establish a new subcommittee titled the "Countering Foreign Influence Subcommittee" to provide recommendations regarding the following issues surrounding foreign influence campaigns:

The Countering Foreign Influence (CFI) Subcommittee will explore the evolving range of foreign influence threats against the United States and identify additional opportunities to counter them within DHS authorities. The subcommittee's mandate will include, but is not necessary limited to, the following issues:

Provide an assessment of all DHS entities that currently have equities in countering foreign influence.

Identify additional DHS entities at the Headquarters and Component levels that have perceived capabilities in countering foreign influence.

Identify the current nation states and illicit groups involved in foreign influence campaigns and provide a forward-looking assessment of their perceived capabilities in conducting future influence campaigns. This assessment should include recommendations on how DHS can best prepare for perceived future foreign influence campaigns.

Provide an assessment of private sector entities and infrastructure that are targeted by foreign influence campaigns and identify support mechanisms and oversight capabilities that DHS has to assist these entities.

These recommendations are due to the full Council no later than 180 days from the date of the subcommittee's formation.

Thank you, in advance, for your work on these recommendations.

APPENDIX C – SUBJECT MATTER EXPERTS

Chris Anderson, Chief of PSHSB's Operations and Emergency Management Division, Federal Communications Commissioners

Nate Blumenthal, Director for DHS Countering Foreign Influence Task Force, CISA

Graham Brookie, Director and Managing Editor, Digital Forensic Lab, The Atlantic Council

Roque Caza, Assistant Director, NTC Counter Network Division

C. W. Diorio, Special Agent, HSI Cyber Crimes Center (C3)

Tim Hemker, Operations Chief, HSI International Operations

Kevin Kane, Public Policy Manager at Twitter

David Magdycz, Division Chief, HSI International Operations Division

Laura Rosenberger, Director and Senior Fellow, Alliance for Securing Democracy, German Marshall Fund of the United States

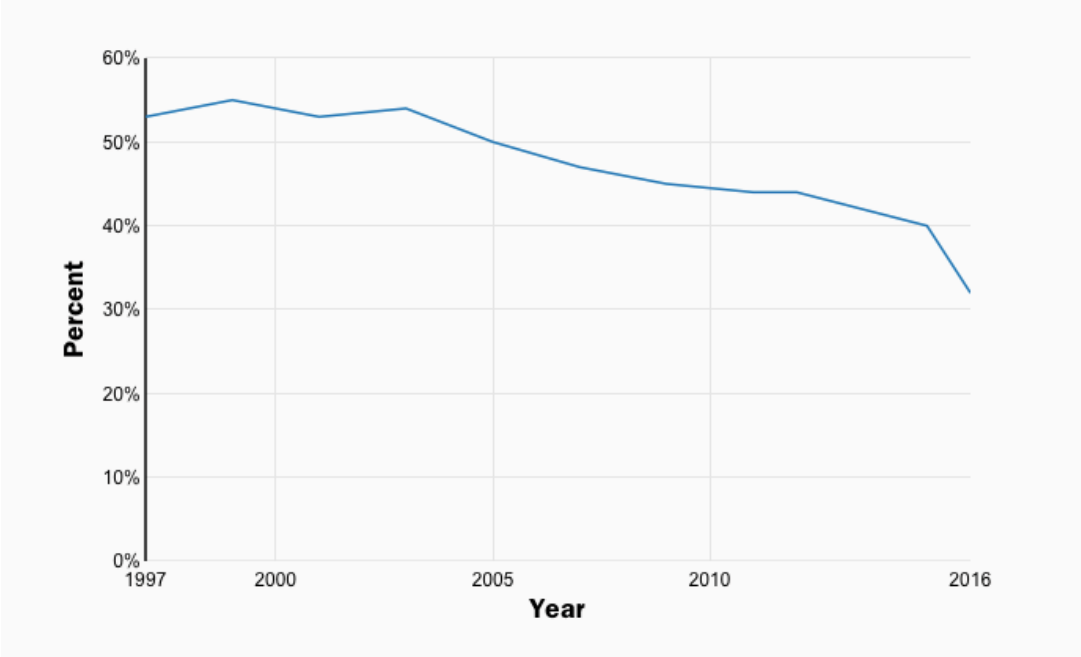
Saleela Salahuddin, Cybersecurity Policy Manger at Facebook

Brian Scully, Deputy Director for DHS Countering Foreign Influence Task Force, CISA

Brian Sterling, Section Chief (Acting), Security, Intelligence, and Information Policy Section, Office for Civil Rights and Civil Liberties, DHS

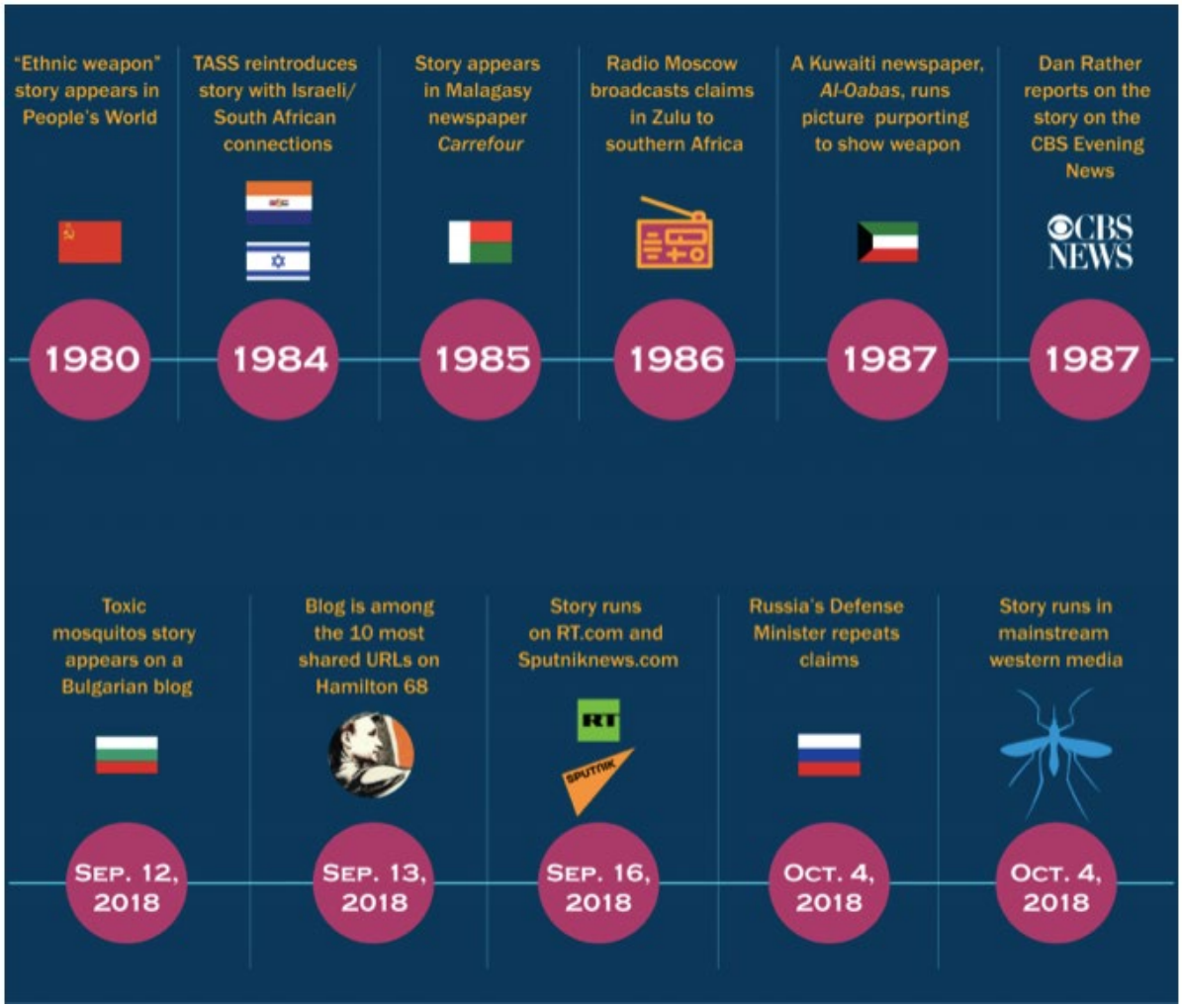
APPENDIX D – FIGURES AND GRAPHS

GRAPH 1 – Public Trust in Traditional News Media, 1997-2016



Source: Brookings Institution (2017)

FIGURE 1 – A Comprehensive Timeline of the Spread of anti-American Rumors Before and After the Advent of Social Media.



Source: Alliance for Securing Democracy (2018)

FIGURE 2 - Example of Russian "bot" Account Activity

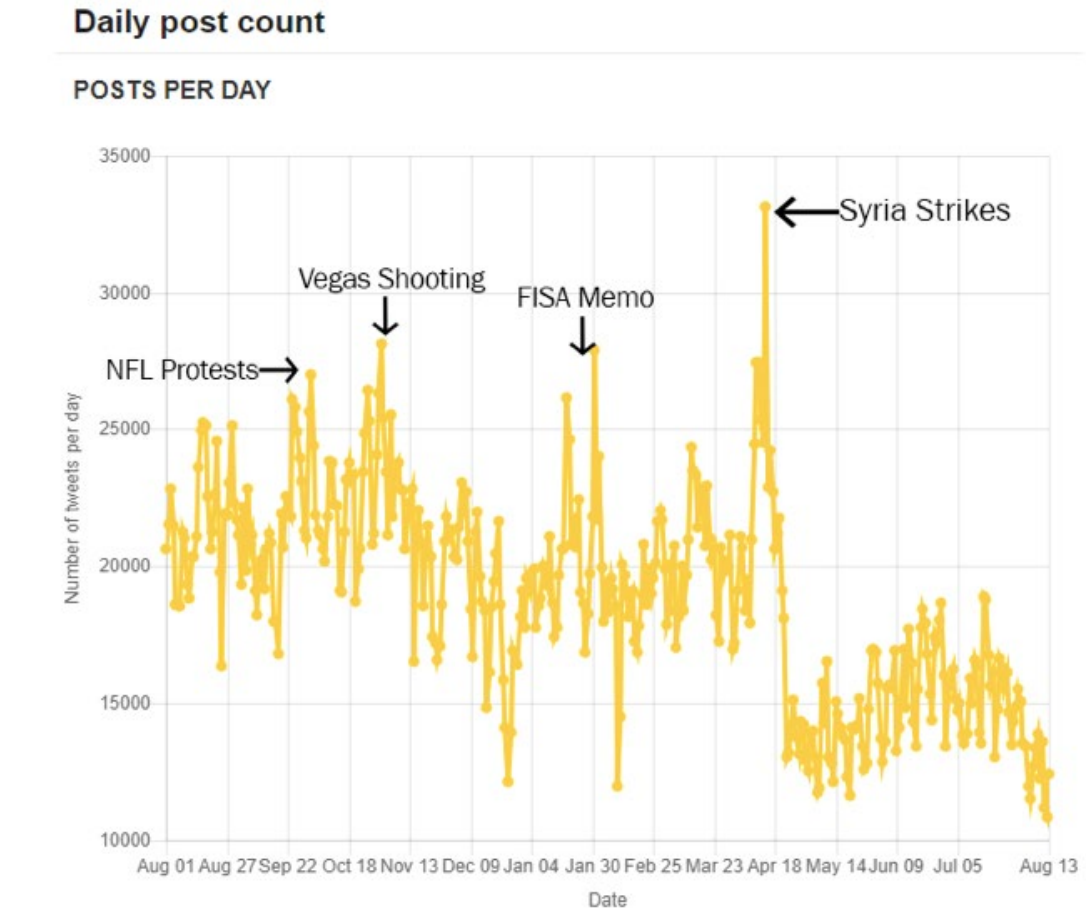


Figure 7 – Daily activity on Hamilton 68 with "spike" days labelled. Again, it is worth reiterating that the decline in May 2018 was due to the manual removal of repurposed bot accounts and is not an indication of reduced activity.

Source: Alliance for Securing Democracy (2018)

APPENDIX E – REFERENCES

"Alternative Reality." *The Economist*, May 30, 2015. https://www.economist.com/europe/2015/05/30/alternative-reality.

Axelrod, Tal. "FBI Chief: Foreign Influence Campaigns Continually Targeting US." *The Hill*, March 5, 2019. https://thehill.com/policy/national-security/432776-fbi-chief-foreign-influence-campaigns-continually-targeting-us.

Bayer et al. "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States," Policy Department for Citizens' Rights and Constitutional Affairs, The European Parliament. http://aei.pitt.edu/97042/1/disinformation_and_propaganda.pdf.

Chen, Adrian. "The Agency." *The New York Times*, June 2, 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

"China's Global Information and Influence Campaign." Council on Foreign Relations. https://www.cfr.org/project/chinas-global-information-and-influence-campaign.

Civil Liberties Perspective on Countering Foreign Interference, DHS Office for Civil Rights and Civil Liberties, April 2019.

"Cyber Threats to Elections: A Lexicon." Office of the Director of National Intelligence. https://www.dni.gov/index.php/ctiic-features/2620-cyber-threats-to-elections-a-lexicon.

"DHS and Facebook Update Election Officials on Foreign Interference Operations." Department of Homeland Security, August 6, 2018. https://www.dhs.gov/news/2018/08/06/dhs-and-facebook-update-election-officials-foreign-interference-operations.

DHS Election Infrastructure Security Resource Guide, National Protection and Programs Directorate, Department of Homeland Security, July 10, 2018. https://www.dhs.gov/sites/default/files/publications/Election%20Resource%20Guide%20July%2018_FINAL%20-%20508.pdf

"Election Security Resource Library." Department of Homeland Security, June 13, 2018. https://www.dhs.gov/publication/election-security-resource-library.

Fly, Jamie M., and Laura Rosenberger. "The Mueller Report Shows Politicians Must Unite to Fight Election Interference," April 22, 2019. https://www.foreignaffairs.com/articles/2019-04-22/mueller-report-shows-politicians-must-unite-fight-election-interference.

Fly, Jamie, Laura Rosenberger, and David Salvo. "Policy Blueprint for Countering Authoritarian Interference in Democracies." Alliance for Securing Democracy, June 26, 2018. http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

"Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," October 27, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Grace, Abigail. "China's Influence Operations Are Pinpointing America's Weaknesses." *Foreign Policy*. October 4, 2018. https://foreignpolicy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses/.

"Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," October 19, 2018. https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections.

Kendall-Taylor, Andrea, and David Shullman. "How Russia and China Undermine Democracy," October 2, 2018. https://www.foreignaffairs.com/articles/china/2018-10-02/how-russia-and-china-undermine-democracy.

Kinzinger, Adam. "All Info - H.R.5181 - 114th Congress (2015-2016): Countering Foreign Propaganda and Disinformation Act of 2016." Webpage, May 10, 2016. https://www.congress.gov/bill/114th-congress/house-bill/5181/all-info.

Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *The Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

Polyakova, Alina. "What Do Russian Disinformation Campaigns Look like, and How Can We Protect Our Elections?" *Brookings*, October 3, 2018. https://www.brookings.edu/blog/brookings-now/2018/10/03/what-do-russian-disinformation-campaigns-look-like-and-how-can-we-protect-our-elections/.

"Report On The Investigation Into Russian Interference In the 2016 Presidential Election", U.S. Department of Justice, March 2019. https://www.justice.gov/storage/report.pdf.

RUSSIA INVESTIGATIVE TASK FORCE HEARING WITH SOCIAL MEDIA COMPANIES, § Permanent Select Committee on Intelligence (2017). https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Transcript-20171101.pdf.

"Russia, Trump, and the 2016 U.S. Election." Council on Foreign Relations. https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Schafer, Bret. "A View from the Digital Trenches – Lessons from Year One of Hamilton 68." Alliance for Securing Democracy, November 19, 2018. http://www.gmfus.org/publications/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68.

United States of America v. Elena Alekseevna Khusyaynova (Eastern District of Virginia September 28, 2018).

"Update on Twitter's Review of the 2016 US Election." https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.

West, Darrell M. “How to Combat Fake News and Disinformation.” *Brookings*, December 18, 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

Williams, Rush Doshi and Robert D. “Is China Interfering in American Politics?” *Brookings*, October 2, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/.

Wilson, Darren. “Situation Report.” Ferguson, Missouri: Federal Bureau of Investigation, August 20, 2014. https://ccrjustice.org/sites/default/files/attach/2018/03/FBI%20881.pdf.

Wright, April. “Deepfakes and Deep Video Portraits — What Are They and What Is the Difference?” *Medium* (blog), January 6, 2019. https://medium.com/@aprilcwright/deepfakes-vs-deep-video-portraits-what-are-they-and-what-is-the-difference-24b7ac538090.

APPENDIX G – GLOSSARY OF ACRONYMS

AI	Artificial Intelligence
C3	Homeland Security Investigations Cyber Crimes Center
CFI	Countering Foreign Influence
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DFT	Deep Fake Technology
DVP	Deep Video Portrait
EIS	Election Infrastructure Subsector
FI	Foreign Interference/Influence
GCC	Election Infrastructure Subsector Government Coordinating Council
HIS	Homeland Security Investigations
HSAC	Homeland Security Advisory Council
IA	Information Activities
I&A	Office of Intelligence and Analysis
IRA	Internet Research Agency
NSA	National Security Agency