Social Media as A National Security Threat Vector

How the Russians attacked America by spreading propaganda through Social Media

John McFarland

DECEMBER 13TH 2017

Abstract

Social Engineering is a significant threat to modern society, and social media has opened new cyber threat vectors that America must defend against. Due to a combination of domestic conditioning, and new cyber tools that a foreign government can use, the American population was primed to be the victims of a cyberoperation that let Russia socially engineer their support for a Russian agenda. Together, the social media environment, the political environment of 2016, and the unique nature of social media environments paint an interesting picture of social media as a National Security Threat Vector in the 21st century, and how Russia used that threat vector to attack American citizens.

Section 0: Introduction

I think; therefore, I am; but does what I think determine who I am? If so, does the information I consume define me? It is with these questions in mind that propagandists wage an information war against their enemies. If one nation can control the information that another nation consumes, they can control the spirit of that nation. This is exactly what happened during the 2016 Presidential election, when Russia used Social Media to shape the reality of hundreds of millions of Americans. Russia's propaganda efforts helped create and amplify a racial and economic divide along partisan lines, and through that shaped reality for those affected. Unlike the public perception of a cyberattack this was not a vulnerability in a computer system that was exploited, it was a vulnerability in our culture that was exploited through social engineering.

Social Engineering is an attack vector that relies on exploiting an individual with the goal of manipulating that person into engaging in a specific action; typically divulging personal or confidential information. In the context of information security

and risk, an employee that is being socially engineered is another point of failure for a risk management team to consider. Willis Towers Watson claims “that two-thirds of cyber breaches are caused by employee negligence or malfeasance including losing laptops, or the accidental disclosure of information” (McAndrew, "Empowered employees: The frontline against cyber threats", 2017). Taken through the lens of National Security, social engineering becomes a lot more dangerous. Hostile states have engaged in propaganda campaigns against each other with the goal of socially engineering entire populations. They do this to shape public sentiment about a conflict that would make their enemy easier to defeat. The best modern example of this is the Russian propaganda campaign to influence the 2016 Presidential election.

While the investigation into the Russian propaganda efforts to influence the 2016 presidential election are still ongoing, there are some clear facts that have already been established. Russia was clearly the threat actor trying to undermine a democratic election for United States President. They worked to undermine this election through several attack vectors. These attack vectors included but were not limited to spreading misinformation through social media (Fandos, Kang, & Isaac, House Intelligence Committee Releases Incendiary Russian Social Media Ads, 2017), cyberattacks on voter rolls in key states (Calabresi, "Russian Hacking on Election More Widespread Than Reported", 2017), and stealing private communications from the DNC (DHS & FBI, "GRIZZLY STEPPE – Russian Malicious Cyber Activity", 2016). Their primary goal was to get a candidate elected that would relieve the Magnitsky Act sanctions placed against them by the Obama administration. Their secondary goal was to diminish the standing

of democracy as a system of government, so they could undermine the United States soft power on the world stage.

Section I: The Social Media Environment

Discussing how Russian operatives used social media to spread propaganda requires an understanding of social media itself. Social media sites are websites that allow communities to grow and communicate using internet technologies. Each individual social media site is distinct in their approach to these connections and communities, but they all use an algorithmic approach to connecting people with similar interests and ideologies. By taking advantage of these algorithms, Russia was able to maximize the potential width of their propaganda efforts while spending the minimum amount of money. Additionally, these platforms have tools for advertisers to "boost" their advertisements so that they reach more social media users.

The Russian social media campaign was extensive and covered several social media sites. Russian operatives masqueraded as regular users on every app they could find a base on. Some of these operations took place within troll communities like 4ochan, but the most effective propaganda was spread through Facebook, Twitter, and Reddit. Each of these offers a different service for a social media user, and Russia used each one for a different purpose. For Facebook, Russia took advantage of the personal atmosphere Facebook creates by reaching out through private messages and user created groups. This allowed them to gain the trust of various users, and take advantage of that trust to convert these users into unwitting agents that would help spread the propaganda for them. For Twitter, Russia relied on overwhelming legitimate news

sources with fake news. Russia played a numbers game, and because Twitter is a more public open forum that many political analysts use to keep a general view of public opinion Russia was able to convince large amount of people that fake events were taking place. Russia used large botnets to obscure the truth with misinformation to manipulate public opinion. For Reddit, Russia built communities that allowed users to congregate together and share ideas. Reddit allows for the creation of themed communities, and Russia harnessed alt-right groups as a nexus of misinformation, which allowed them easy access to premade communities.

To understand how Russia uses social media to propagate misinformation throughout the internet, there needs to be an understanding of how social media uses algorithms to display content. While every site uses its own proprietary algorithm, they are all based around a simple premise; show content that keeps a user coming back. When a post is made, the social media site treats this post object as something to categorize, rank, and present. A post that has been shared or liked by many users is ranked higher, and therefore shown to more people eligible to see it. A post also considers the relationship between the poster and the view, as well as the time since the content was posted. This type of presentation allows a social media site to show their users the most popular content at any given time, but it also severely restricts the content a use will see. Users who consistently like or interact with a certain type of content will start to see that content more frequently on their feed. This creates a bubble, where a user's view of events can become skewed or manipulated. "That's where the algorithms come in. American researchers have found they can use mathematical formulas to segment huge populations into thousands of subgroups

according to defining characteristics like religion and political beliefs or taste in TV shows and music. Other algorithms can determine those groups' hot-button issues and identify "followers" among them, pinpointing those most susceptible to suggestion. Propagandists can then manually craft messages to influence them, deploying covert provocateurs, either humans or automated computer programs known as bots, in hopes of altering their behavior." (Calabresi, "Russia's US Social Media Hacking: Inside the Information War", 2017) These bubbles are dangerous and create spaces where a user's preconceived beliefs can be supported through confirmation bias.

Like an organic environment that serves as a natural host to disease and parasites, once these bubbles are created they can become home to malicious users seeking to spread false information for a goal. Malicious users or groups will buy ads on the platform of their choice, and will serve those ads to a group they are trying to infect. Users will see these ads, and share them, creating a free publicity boost, and ensuring that more users see this malicious content. Compared to traditional propaganda efforts, this method is a lot cheaper. It allows for more information to be spread to a wider audience for less money.

One of the ways social media mitigates that risk is through a process called verification. Verification is a process by which social media sites authenticate public figures, bands, and companies to prevent other accounts from fraudulently impersonating them. Traditionally this has been used to ensure security to a brand's integrity, but in the current political climate it also adds authority to their opinions or beliefs.

Verification isn't enough to stop misinformation from spreading. One of the central themes of Russian active measures on social media is a mistrust of authority, and often users who have been compromised by Russian propaganda will ignore the verification symbol of someone who presents facts that are fatal to the user's beliefs. Often these users will instead share information from meme accounts, which use humor and satire to undermine the credibility of political opponents. The meme format is perfect for this goal because it allows a complex idea to be conveyed to an uneducated and vulnerable audience without them feeling spoken down to or lectured. This is important because the victim doesn't consider the message's intent since they feel included in the joke, and therefore they internalize a part of that message as a cultural identity.

Section II: The Political Environment and Cultural Threat Vectors

The vulnerabilities in a program are often dependent on the operating system the program is running on. The threat vectors used by Russia during their assault on American voters during the 2016 election were only available because of the political environment of the country. Thirty years of conservative propaganda and polarization created an authoritarian population without the ability to think critically. While originally these victims were used as a means of passing tax cuts and deregulation for special interests, during the 2016 election Russia took advantage of them to push a pro-Russia agenda masked as conservatism through American politics.

Many experts consider the 2016 election to be a referendum on America's role as leader of the post WWII global order. Americans voted to recede from the world stage, and in doing so opened the world back up to multipolar order. America destroyed its

own hegemony. Many consider this the natural path of a unipolar world, but when examined closely a pattern emerges. Behind every movement that helped contribute to this, Russia had influence.

Before Russian active measures against the American population can be discussed, the domestic propaganda campaign that the right wing waged on its own constituents needs to be examined. The Republican effort to propagandize their constituents goes back to a memo from the Nixon administration where Roger Ailes detailed a plan to put the GOP on TV. “A memo entitled “A Plan for Putting the GOP on TV News,” buried in the Nixon library details a plan between Ailes and the White House to bring pro-administration stories to television networks around the country. It reads: “Today television news is watched more often than people read newspapers, than people listen to the radio, than people read or gather any other form of communication. The reason: People are lazy. With television you just sit—watch—listen. The thinking is done for you” (Bell, "Richard Nixon and Roger Ailes 1970s plan to put the GOP on TV", 2011) The goal was simple; tell people what to think instead of giving them the ability to think for themselves. This approach to media didn’t end in the Nixon era, and when Roger Ailes was given the CEO position of Fox news in 1996, he brought it with him. In the 21 years since Fox News launched, they have become increasingly more partisan, going from an organization that presented facts poorly to an organization that manufactured outrage and served as a cover for right-leaning political operatives.

This type of concentrated effort would not have been possible if their relationship with conservative politicians was not symbiotic. The Republican political playbook values victory above all else, and Republicans make no effort to mask that those who do

not vote Republican aren't a priority in their legislation. It is no secret that party affiliation has roots in the education level of a person. "Recent Pew Research Center studies also have found increasing differences in party identification between those with more and less education. And there is a growing ideological divide between these groups, with highly educated adults holding increasingly liberal attitudes across a range of issues." (Suls, "Educational divide in vote preferences on track to be wider than in recent elections", 2016) To a Republican, this means that college educated Americans are the enemy, and should be converted or disenfranchised. What this also means is that the constituency views having an education as something "liberal" or "elitist". This became a cultural staple of the Republican party and its conservative constituents. Through the lens of a protected computer system we can view this as something that intentionally cripples a firewall's ability to protect a network from malicious software. By stripping the security system of security definitions, it can no longer identify a threat, therefore they leave the computer system vulnerable. Similarly, by stripping their constituents of the ability to think critically, the GOP left their base vulnerable to malicious actors who used the same information channels to send misinformation that coopted the Republican party for Russian interests.

Through dog whistles and obscurity, Republicans changed the truth to fit their narrative, and fed an ignorant base any talking point that served them best at the time. This is most clearly seen when it comes to race. Lee Atwater said it best:

> "You start out in 1954 by saying, "Nigger, nigger, nigger." By 1968 you can't say "nigger"—that hurts you, backfires. So you say stuff like, uh, forced busing, states'

> rights, and all that stuff, and you're getting so abstract. Now, you're talking about cutting taxes, and all these things you're talking about are totally economic things and a byproduct of them is, blacks get hurt worse than whites.... "We want to cut this," is much more abstract than even the busing thing, uh, and a hell of a lot more abstract than "Nigger, nigger."". (Perlstein, "Exclusive: Lee Atwater's Infamous 1981 Interview on the Southern Strategy", 2015)

Like most authoritarian groups, the Republican party has masked the intent of their propaganda with a positive spin. Instead of discussing civil rights, the Republican party would discuss states' rights. Instead of actively attacking people of color, the Republican party would focus on economic issues that passively disenfranchised undesirable groups. When the 2016 Presidential election came up, Russia was ready to take advantage of this primed authoritarian group by using the same information channels Republicans used. Russia used Republican groups across social media to serve race flavored political propaganda that riled conservatives, and then endorsed a pro-Russian candidate that would alleviate those fears. Russia made a problem seem massive, and then offered Americans a solution with their chosen candidate. This type of propaganda was natural to the Russian regime, as it had a century of experience pushing pro-Russian propaganda to former Soviet client states. (Starr, "Opinion | How Putin's Russia uses Soviet-era tricks to evoke racist white fears", 2017)

The final component necessary to discuss how Republicans set the stage for Russian interference comes in the form of legislation passed dealing with our first amendment. In the United States v. FEC, "The United States Supreme Court held (5–4)

on January 21, 2010 that the free speech clause of the First Amendment to the Constitution prohibits the government from restricting independent expenditures for communications by nonprofit corporations, for-profit corporations, labor unions, and other associations." (Wikipedia, "Citizens United v. FEC") This decision seems like a domestic issue, and has been cited as one of the primary causes of income inequality in America, but there is a more insidious repercussion that needs to be addressed in conjunction with Russia's social media efforts. Title 52 USC 30121 strictly limits the amount of support a foreign entity can give a domestic campaign. ("52 U.S. Code § 30121 - Contributions and donations by foreign nationals") This is to prevent a US politician from considering foreign governments one of their constituents. The Republican-supported 'Citizens United' ruling helped destroy that safety valve by allowing domestic corporations to pour as much money as necessary into domestic elections. This meant that any foreign government who wanted to pour massive amounts of money into our election could form a shell company, and use that company to fund a candidate. Republicans pushed this as a way to allow private individuals to wage a political war against opponents of the Republican party, but Russia used this as a way to circumvent every security control for foreign money in American elections. Russia used shell companies to buy advertisements on social media supporting a presidential candidate that supported their interests.

With the environment ripe for abuse from years of Republican efforts to undermine American democracy, the stage was set for Russia to assert their influence through coordinated cyberattacks, propaganda efforts and data dumps. America was left

defenseless after being pillaged by politicians who spent their entire lives lining their own pockets at the expense of American security.

Section III: Threat Vectors and Where to Find Them

In an information war, the ability to spread information is key. Social media is the most viable theater of combat for any malicious actor who wants to socially engineer large portions of the population. The largest threat vectors during the 2016 Presidential election were Facebook, Twitter, and Reddit. By using fake accounts, meme groups, buying advertisements, and creating fraudulent news sources Russia was able to use these platforms to spread misinformation and socially engineer the American public into electing a President who served their interests. This happened differently on each platform.

For Facebook, Russia took advantage of user groups to socially engineer users who thought they were in 'good company'. As normal users created groups to indulge in their interests, Russia created fake accounts to take advantage of those groups to serve propaganda. According to a Senate Intelligence hearing where Facebook representatives testified, as many as 126 million people saw material posted by a Russian troll farm under fake Facebook identities between 2015 and 2017. This means that over 50% of American voters were exposed to Russian propaganda during the 2016 presidential election. (Weise, "Russian fake accounts showed posts to 126 million Facebook users", 2017)

Russian fake Facebook accounts are expert forgeries designed to infiltrate specific groups. Using psychological profiles of American citizens, Russia mass-produced

identities based on the character models of the groups they wanted to infiltrate. Additionally, they created profiles specifically to create and share bought advertisements. "Most of the 3,000 ads did not refer to particular candidates but instead focused on divisive social issues such as race, gay rights, gun control and immigration, according to a post on Facebook by Alex Stamos, the company's chief security officer. The ads, which ran between June 2015 and May 2017, were linked to some 470 fake accounts and pages the company said it had shut down." (Shane & Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads", 2017)

These ads were not bought just to sway the political opinions of average Americans. These ads were part of a microtargeting campaign that targeted specific districts in important swing states to ensure that Russia's candidate got elected. "Some of the Russian ads appeared highly sophisticated in their targeting of key demographic groups in areas of the states that turned out to be pivotal, two of the sources said. The ads employed a series of divisive messages aimed at breaking through the clutter of campaign ads online, including promoting anti-Muslim messages" (Raju, Byers, & Bash, "Exclusive: Russian-linked Facebook ads targeted Michigan, Wisconsin", 2017) In the same source, we see the impact of these efforts. "Michigan saw the closest presidential contest in the country -- Trump beat Democratic nominee Hillary Clinton by about 10,700 votes out of nearly 4.8 million ballots cast. Wisconsin was also one of the tightest states, and Trump won there by only about 22,700 votes. Both states, which Trump carried by less than 1%, were key to his victory in the Electoral College."

Russia used their army of fake accounts to take advantage of Facebook's algorithm for sharing content by spreading these ads in a way that increased their edge

ranks. This abuse of Facebook's algorithm allowed Russia to spend the minimum amount of money to reach a larger breadth of users.

> "They had taken advantage of Facebook's algorithm, something Lior Abraham, founder of behavior analytics company Interana and former Facebook engineer, never anticipated when he helped create the news feed. Abraham had worked at Facebook between 2007 and 2013, developing key functions on the news feed, as well as creating a data analytics tool called Scuba that the social network still uses. When he helped build the news feed, the goal was always to promote engagement with your friends and family, and not political discourse. "We would just give priority to break-up stories and photos at the time," Abraham said. Through the years, the algorithm would get tweaked to include more artificial intelligence and less of a human touch. But the focus on engagement pushed arguments to the forefront, creating a news feed that Abraham can hardly recognize anymore. "It's contrary to the original mission of creating communities," Abraham said. "You're just dividing larger communities." So, if you've noticed your Facebook feed getting more negative, that's because its algorithm has been promoting arguments, Whelan said. And with the rise of bots, and trolls getting more sophisticated, it's becoming harder to tell if that person you're arguing with is even real." (Ng, "How Russian trolls lie their way to the top of your news feed", 2017)

This allowed Russia to simulate the environments necessary for their operations to grow. By creating fake news, using fake accounts to buy advertisements to push fake news, and putting it in places where conflict would help it be seen, Russia managed to increase viewer imprint and ensure that they got the maximum mileage for the least amount of money. When stories wouldn't gain traction, they would create conflict to make sure the process gained ground.

Russia's efforts on Facebook would not have gained ground if it wasn't for the "useful idiots"(Wikipedia, "Useful idiot"). The term "Useful Idiot" was attributed to

Vladimir Lenin. It described someone who unknowingly helped the Soviets spread communism. In the information era it has taken on a new meaning as social media users unknowingly spread Russian propaganda against the United States. Facebook users, political operatives, and Presidential candidates would parrot narratives being used by Russia to discredit America. This gave those fraudulent news sources the authenticity and authority they needed to be accepted into an uneducated American population.

Russia followed a similar strategy on Twitter, but the less personal nature of Twitter allowed them to automate several of the mechanisms they used to propagate fake news. Twitter offered the opportunity to use botnets to spread messages, which required a lot less personalization to propagate a message. To understand how Russians took advantage of the Twitter algorithm there needs to be an understanding of Botnets, and their role on the Twitter platform.

Botnets are a collection of automated processes or "robots" that form a network that is directed by a command and control server. While botnets have many uses, in this context they are used to push any message the owner of the botnet wants to spread. During the 2016 presidential election this weapon was used to influence social media opinions on Twitter. Security expert Brian Krebs noticed a trend. "Krebs explains that further investigation determined that almost all of the new Twitter followers he had gained were actually part of a social media botnet being used to falsely amplify propaganda and fake news posts, and to intimidate journalists, activists and researchers. "The botnet or botnets appear to be targeting people who are exposing the extent to which sock puppet and bot accounts on social media platforms can be used to

influence public opinion."" (Bradley, "Pro-Kremlin Botnets Pose An Existential Threat To Twitter", 2017)

The Russian botnets targeted anyone who had a dissenting opinion. Using data analytics to parse tweets, and machine learning to create word associations, a botnet could target and respond to any topic; overwhelming legitimate commentary with propaganda in a manner of minutes. “The network’s main role is to amplify messages deemed to benefit the Kremlin, but that doesn’t mean the websites' authors share the same goals, said Laura Rosenberger, director of the Alliance for Securing Democracy, which created the monitoring project for the fund.” (Hafner, "OnPolitics Today: How Russian Twitter accounts push pro-Trump propaganda", 2017)

These tactics are useful for spreading misinformation and controlling the news cycle, but they would be ineffective without normal users helping to share this information. Like Facebook, Twitter propaganda is heavily reliant on useful idiots. However, Twitter had a much more powerful amplification tool; Donald Trump. The President-elect was a lighting rod for controversy, and as such was able to attract a lot more attention to misinformation he helped share from his account. "He denies the intel from the United States about Russia. He claimed that the election could be rigged; that was the number one theme pushed by RT Sputnik news," Watts said. "So part of the reason active measures works and it does today in terms of Trump Tower being wiretapped is because they parrot the same lines." (Stracqualursi & Kelsey, "Trump's campaign tactics, trolls strengthened Russia's election meddling, expert says", 2017) This powerful tool helped bring Russian active measures into American politics, and a repercussion of that was that Russians got to push their agenda to Americans. Donald

Trump created a threat vector for Russian cyber propaganda efforts, and increased the risks to American infrastructure because of it.

It is impossible to have a conversation about Russian active measures as a cybersecurity threat without discussing Reddit as a simulated command and control server for hosted content. If Facebook is the heart to heart conversation between two family members, and Twitter is the intercom those family members use to keep tabs on each other, then Reddit would be the house they lived in. The self-proclaimed "Front page of the internet" is a one stop shop for any type of demographic a Russian operative could look to target.

Unlike both Facebook and Twitter, Reddit doesn't need fake accounts because Reddit has no expectation of identity. The obscurity of the Reddit username gives the perfect cover for Russian operatives to infiltrate the different communities as individual users. Following the trend of using conservative groups to serve Americans malicious information, Russian bots infiltrated a subreddit dedicated to the President.

American Senators have taken notice. "According to The Hill, Warner is interested in examining if Russia used Reddit for social media influence. Experts note that several hoax stories caught fire on the site. For example, as *The New York Times* shows, just four hours after someone posted on Twitter about anti-Trump protestors being bussed into Austin, the tweet was posted to Reddit, where it was quickly "upvoted" (Reddit's version of users liking a post) by users. Nine hours later the story made its way to Facebook where more than 300,000 people shared it. The busses were, in fact, part of a corporate conference." [Fortune source] The New York

times is not the only organization to take notice of Reddit's use as a threat vector for Russian cyberoperations. Samantha Bradshaw of Oxford University noted it as well. In her studies of Russian propaganda, she sees Reddit as a perfect biome for threat vectors to grow organically. "[Reddit] is one of the forums that some of the coordinated information campaigns happened on," says Samantha Bradshaw, a researcher at Oxford University who has studied how governments use social media to influence public opinion. Bradshaw says that she's witnessed patterns on the site that suggest a deliberate effort to distribute false news." (Breland, "Warner sees Reddit as potential target for Russian influence", 2017)

These three social media sites served as both the environment to launch attacks, and the tool to launch them with; but they aren't the only ones. Nearly every social media site was compromised in some way. As each social media site offers a unique experience to their users, Russia gets a unique method of delivery for their propaganda. As Americans wake up to social media as a cybersecurity threat vector, this game of cat and mouse will evolve and become more elaborate.

Section IV: Defending our Freedoms without losing them.

The hardest challenge facing cybersecurity experts who want to defend against Russian cyberoperations is the American constitution. The first amendment gives the explicit right of protection from the government stifling speech. This makes the government's job hard, as it must balance a fair and free society with the need to defend themselves. The American government has a few options available to it, but the road ahead is difficult.

Senator Mark Warner (D), Senator John McCain(R), and Senator Amy Klobuchar(D) think that the best way to go forward is through regulation. “First and foremost, this is an issue of national security – Russia attacked us and will continue to use different tactics to undermine our democracy and divide our country, including by purchasing disruptive online political ads. We have to secure our election systems and we have to do it now – the next election is only 383 days away,” Senator Klobuchar said. “This bipartisan legislation would help protect our democracy by updating our laws to ensure that political ads sold online are covered by the same rules as TV or radio stations – and make them public so Americans can see who is trying to influence them(Klobuchar, Warner, & McCain, "Klobuchar, Warner, McCain Introduce Legislation to Improve National Security and Protect Integrity of U.S. Elections by Bringing Transparency and Accountability to Online Political Ads", 2017) This legislation would require social media sites to be transparent about who is buying ads, and would bring social media advertising regulation closer to the way other entertainment advertising is done.

While this method may be affective, social media sites want to go a step further and perhaps get ahead of the legislation. “As part of its ongoing transparency efforts on Russian activity, Facebook today revealed that it will soon let users find out if they liked or followed pages created by the Internet Research Agency between January 2015 and August 2017. The company said it plans to roll out the tool by the end of this year, which is going to live in the Facebook Help Center and will also include information about Instagram accounts.” (Alvarez, "Facebook will alert you if you liked a fake Russian

account", 2017) By engaging Russian misinformation at the source social media companies can borrow tactics used by the intelligence community in fighting terrorism.

On a more personal level, every citizen needs to be vigilant. Ultimately a user is responsible for the information that they consume. If they go to a site that has a large alt-right demographic, they should expect to be served content that reinforces alt-right views. Similarly, if they go to a site with a large left leaning demographic, they should expect to be served content that reinforces left leaning views. This is the nature of private clubs where people come together to congregate with similar interests and hobbies. A user needs to apply the same safety standards that society once expected in public. “Don’t trust everything you see on TV” became “Don’t trust everything you read on the internet”. A user needs to verify information before they accept it as a truth.

Section V: Conclusion

Propaganda has taken a new form in the 21st century, and cybersecurity experts are on the front lines defending against it. With Social media as a tool, foreign propagandists can push new narratives in real time to a vulnerable population. As these new threat vectors open, experts must be vigilant in their defense of democracy. Experts must also be willing to fight back. As Clint Watts noted in his senate interview “Cyber on cyber, it feels like we’re in a glass house throwing rocks at a mud hut” ("Senate Intelligence Hearing", 2017) The nature of Russian media as an institution makes it hard for America to use the same subversive tactics against Russia. As such, American cybersecurity experts need to be proactive in spreading their own propaganda that bolsters American interests. If we are negligent, we will become negligible.

References

52 U.S. Code § 30121 - Contributions and donations by foreign nationals. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/52/30121

Alvarez, E. (2017, November 23). Facebook will alert you if you liked a fake Russian account. Retrieved from https://www.engadget.com/2017/11/22/facebook-russia-transparency-tool/

Bell, M. (2011, July 01). Richard Nixon and Roger Ailes 1970s plan to put the GOP on TV. Retrieved from https://www.washingtonpost.com/blogs/blogpost/post/richard-nixon-and-roger-ailes-1970s-plan-to-put-the-gop-on-tv/2011/07/01/AG1W7XtH_blog.html

Bradley, T. (2017, August 31). Pro-Kremlin Botnets Pose An Existential Threat To Twitter. Retrieved from https://www.forbes.com/sites/tonybradley/2017/08/31/pro-kremlin-botnets-pose-an-existential-threat-to-twitter/

Breland, A. (2017, September 27). Warner sees Reddit as potential target for Russian influence. Retrieved from http://thehill.com/policy/technology/352584-warner-sees-reddit-as-potential-target-for-russian-influence

Calabresi, M. (2017, June 22). Russian Hacking on Election More Widespread Than Reported. Retrieved from http://time.com/4828306/russian-hacking-election-widespread-private-data/

Calabresi, M. (2017, May 18). Russia's US Social Media Hacking: Inside the Information War. Retrieved from http://time.com/4783932/inside-russia-social-media-war-america/

Citizens United v. FEC. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Citizens_United_v._FEC

DHS, & FBI. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved from https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity Reference Number: JAR-16-20296A

Fandos, N., Kang, C., & Isaac, M. (2017, November 01). House Intelligence Committee Releases Incendiary Russian Social Media Ads. Retrieved from https://www.nytimes.com/2017/11/01/us/politics/russia-technology-facebook.html

Hafner, J. (2017, August 24). OnPolitics Today: How Russian Twitter accounts push pro-Trump propaganda. Retrieved from https://www.usatoday.com/story/news/politics/onpolitics/2017/08/24/onpolitics-today-how-russian-twitter-accounts-push-pro-trump-propaganda/600157001/

Klobuchar, A., (D), Warner, M., (R), & McCain, J., (R). (2017, October 19). Klobuchar, Warner, McCain Introduce Legislation to Improve National Security and Protect Integrity of U.S. Elections by Bringing Transparency and Accountability to Online Political Ads. Retrieved from https://www.klobuchar.senate.gov/public/index.cfm/2017/10/klobuchar-warner-mccain-introduce-legislation-to-improve-national-security-and-protect-integrity-of-u-s-elections-by-bringing-transparency-and-accountability-to-online-political-ads

McAndrew, S. (2017, October 5). Empowered employees: The frontline against cyber threats. Retrieved from https://www.willistowerswatson.com/en/insights/2017/10/empowered-employees-the-frontline-against-cyber-threats

Ng, A. (2017, October 30). How Russian trolls lie their way to the top of your news feed. Retrieved from https://www.cnet.com/news/facebook-twitter-social-media-russian-troll-politics-chaos/

Perlstein, R. (2015, June 29). Exclusive: Lee Atwater's Infamous 1981 Interview on the Southern Strategy. Retrieved from https://www.thenation.com/article/exclusive-lee-atwaters-infamous-1981-interview-southern-strategy/

Raju, M., Byers, D., & Bash, D. (2017, October 04). Exclusive: Russian-linked Facebook ads targeted Michigan, Wisconsin. Retrieved from http://www.cnn.com/2017/10/03/politics/russian-facebook-ads-michigan-wisconsin/index.html

Senate Intelligence Hearing. (2017, March 30). Retrieved from https://www.intelligence.senate.gov/hearings/open-hearing-disinformation-primer-russian-active-measures-and-influence-campaigns-panel-i#

Shane, S., & Goel, V. (2017, September 06). Fake Russian Facebook Accounts Bought $100,000 in Political Ads. Retrieved from https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

Starr, T. J. (2017, October 09). Opinion | How Putin's Russia uses Soviet-era tricks to evoke racist white fears. Retrieved from https://www.washingtonpost.com/news/global-opinions/wp/2017/10/09/how-putins-russia-uses-soviet-era-tricks-to-evoke-racist-white-fears

Stracqualursi, V., & Kelsey, A. (2017, March 30). Trump's campaign tactics, trolls strengthened Russia's election meddling, expert says. Retrieved from http://abcnews.go.com/Politics/senate-committee-probe-russian-meddling-us-election-begins/story?id=46463551

Suls, R. (2016, September 15). Educational divide in vote preferences on track to be wider than in recent elections. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/15/educational-divide-in-vote-preferences-on-track-to-be-wider-than-in-recent-elections/

Weise, E. (2017, November 01). Russian fake accounts showed posts to 126 million Facebook users. Retrieved from https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/

Wikipedia. (n.d.). Useful idiot. Retrieved from https://en.wikipedia.org/wiki/Useful_idiot