SCUSA 71 Table Paper: Weaponization of Information

Social media plays an increasingly important role in American politics: Social justice movements have become synonymous with their hashtags, politicians connect and communicate with their constituents online, and the President’s personal Twitter account is a source of official Government policy.¹ Today, seven-in-ten² Americans use social media for an average of nearly two and a half hours every day.³ This large and politically active community is also an attack surface for hostile actors to influence policy, sow social and political division, erode trust in Western democratic institutions, and recruit extremist sympathizers. This paper will focus on the sophisticated, well-understood, and well-documented instances of Russian influence over social media. This paper will also examine how everyday social media users become radicalized. This paper concludes with a summary of the challenges facing policymakers that seek to regulate weaponized information.

Influencing Policy

Believing that a Trump administration would be a better deal for Russia, Vladimir Putin directed the Internet Research Agency (IRA) and Russian intelligence agencies to interfere in the 2016 U.S. Presidential elections by discrediting candidate Hilary Clinton and supporting candidate Donald Trump.⁴ The Russian effort had three components: hacking political entities, compromising state election systems, and online propaganda.⁵

The Russian online propaganda effort was primarily asserted through thousands of social media accounts impersonating U.S. citizens, activists, companies, and political organizations.⁶ The House Intelligence Committee has documented fake Russian accounts on Instagram, Facebook, Twitter, Reddit, Tumblr, Pinterest, Medium, YouTube, Vine, Google+, and others.⁷ To get an idea of the scope, consider the Russian campaign on Facebook alone.⁸

- 470 Facebook pages, such as Blacktivists, United Muslims of America, Being Patriotic, Heart of Texas, Secured Borders, and LGBT United.
- 3,393 paid Facebook advertisements.
- Over 80,000 pieces of organic content.
- Reached more than 11.4 million Americans and over 126 million Facebook users worldwide.

The Internet Research Agency had a budget of over $1.25 million each month to carry out its informational campaigns.⁹ While it is illegal for foreign individuals and governments to spend money to influence US elections, the majority of the IRA budget was used to generate shareable content that could be freely posted. Despite indictments brought against Russian agents for campaign interference,¹⁰ it is not clear where the line between foreign influence and free speech lies.¹¹

Russia also uses text messages, real and invented news outlets, videos, websites, trolls, and even direct approaches to human targets to spread its propaganda. Perhaps more troubling than the variety of techniques in the Russian arsenal is the number of actors adopting the Russian playbook. This year alone, Twitter has discovered more than 7,000 fake accounts originating in Iran that are attempting to influence the 2020 U.S. elections.¹²
Sowing Division

Researchers at the University of Washington studying the Black Lives Matter movement on Twitter found that fake IRA-generated accounts were amongst the most retweeted. Russian accounts posted extreme and polarizing content on both sides of the political spectrum. The goal of Russian influence in a U.S. social justice movement is to sow discord by inflaming passions on a range of divisive issues.

According to Homeland Security experts Andrew Weisburd, Clint Watts, and J.M. Berger, Russia targets social tensions by aggrandizing police brutality, racial tensions, protests, anti-government standoffs, and alleged government misconduct in an effort to "undermine the fabric of society." The result is *policy paralysis*: Political division that makes it harder for the United States to conduct foreign policy and to wield its diplomatic and military power in the world.

The former Soviet Union countries, or the *near abroad*, have been the target of divisive Russian social media campaigns for decades. According to the former U.S. Ambassador to Ukraine, "Everyone knows the Kremlin seeks to use information to deny, deceive, and confuse... You could spend every hour of every day trying to bat down every lie, to the point where you don’t achieve anything else. And that’s exactly what the Kremlin wants."

How effective are Russian campaigns to sow division in the U.S.? It is difficult to measure. Jim Pasco, a senior adviser in the nation’s largest police union, says that Russian involvement in the #BlackLivesMatter movement and #BlueLivesMatter countermovement was highly effective. "There is absolutely no doubt that these ad placements further inflamed tensions in already volatile and already sensitive situations at critical times," said Pasco. According to Bret Schafer of the Alliance for Securing Democracy, even if divisive social media content only works 10% of the time, it is still an effective tool for Russia.

While Russian agents did not create the social and political polarization in the United States, they certainly benefit from it and actively work to encourage it.

Eroding Trust

According to Keir Giles, author of NATO’s *Handbook of Russian Information Warfare*, "the received wisdom in Russia is that ‘information confrontation campaigns’ are developed by the West to compromise Russia’s national sovereignty and facilitate regime change." As the leading democratic power, the United States receives the lion’s share of Russia’s contempt for the West. For instance, the Minister of Culture Vladimir Medinskiy promotes the idea that the Netflix video streaming service is financed by the U.S. government as a method of "entering the minds of every inhabitant of the Earth."

To combat the West, Russia erodes trust in democratic and Western institutions. As there is nothing more central to democracy than fair and free voting, undermining trust in the election system is an important objective for the Kremlin. The Senate Intelligence Committee recently released a 69-page report documenting Russia’s attempts to hack into the voting infrastructure in all 50 states prior to the 2016 elections. It likely that Russia’s goal was not to change votes, but to cast doubt over the integrity of the election process in general. An untrustworthy election process undermines the
accountability that officials have to the American public and challenges the legitimacy of the
government.

Russia also takes advantage of Western society’s instinctive distrust in authority by pushing a wide
range of conspiracy theories. Conspiracy theories promote fear of the government while questioning
the expertise of anyone who might calm those fears.27 For instance, #FalseFlag was of the top hashtags
spread by fake Russian accounts after the 2017 Las Vegas mass shooting.28 In another instance,
Russian bots pushed a White House petition to remove George Soros–owned voting machines, which
do not exist, from 16 states. The petition garnered 129,000 signatures.29

Russia also uses automated, partially automated, and human-controlled bots to frame ongoing debates
in a manner favorable to the end state desired by the Kremlin.30 In 2014, a Russian troll army
reportedly flooded The Guardian’s website with 40,000 comments a day promoting a narrative that
an American think-tank plotted with Ukraine to shoot down Malaysia Airlines Flight 17 as part of an
ethnic cleansing conspiracy.31

Once again, it is difficult to assess the efficacy of the Russian strategy. According to Gallup polls, trust
in news media - which Americans believe plays a crucial role in democracy - bottomed out in 2016.32
Trust in Congress is currently at historic lows.33 However, trust in Western alliances has proven
durable despite attempts to discredit them.34 Nonetheless, Russia continues to target democratic
institutions and is making progress in parts of the world.35 The danger posed by Russian propaganda
is still very real. As former NSA scientist and CEO of Immunity Consulting David Aitel puts it, "I
don’t have to blow something up to destroy your country. I just have to reduce trust in your national
way of life.36

Extremist Inculcation

Al Qaeda pioneered the use of social media as platform to advertise their brand of extremism. The
Islamic State proved themselves the true masters social media when they recruited and radicalized an
estimated 40,000 foreign nationals from 110 countries online.37 According to Institute for Strategic
Dialogue, a London-based think-tank, ISIS pivoted to a social media strategy after suffering significant
setbacks on the ground, and now prioritizes propaganda over jihad itself.38

Today, the FBI is combating a new flavor of extremism that is flourishing in the United States:
Antigovernment extremism, such as the far-right conspiracy-peddling organization QAnon.39 These
groups take advantage of social media platforms’ bias for engaging content to nudge users toward
increasingly extreme content.40

Everyday users might not intend to participate in online outrage, much less lead it. But the incentive
structures and social cues of algorithm-driven social media sites like Facebook can train them over
time — perhaps without their awareness — to pump up the anger and fear. Eventually, feeding into
one another, users arrive at hate speech on their own. Extremism, in other words, can emerge
organically.41

These "organically" grown extremists are also violent. A conspiracy theorist opened fire in a D.C.
pizza shop to save children he believed were trapped in a sex-slave ring run by Hilary Clinton.42 A
California man was arrested for conspiring to blow up what he believed to be a satanic temple
monument in the Illinois capital building.\textsuperscript{43} Two men were arrested for stockpiling weapons in a plot to attack a research facility in Alaska they believed was used "to control the weather and prevent humans from talking to God."\textsuperscript{44}

The payoff for peddling conspiracy theories on platforms like YouTube can be huge and providers have little incentive to remove sensational content that keeps users glued to their screens.\textsuperscript{45} While Sundar Pichai, the CEO of Google and YouTube, has promised to "do more",\textsuperscript{46} recent studies suggest it is not working.\textsuperscript{47}

**Regulating Weaponized Information**

There is currently no legislation or policy regulating weaponized information in the United States. Any new regulation would reverse decades of law and doctrine that protects the Internet as a free and open platform. Indeed, the latest \textit{United States National Security Strategy} seeks to maintain "minimal barriers to the global exchange of information" online.\textsuperscript{48}

The most prominent manifestation of the American attitude toward Internet freedoms is Section 230 of the \textit{Communications Decency Act}, often referred to as "the most important piece of Internet legislation ever created":\textsuperscript{49}

\begin{quote}
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider [...] No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.\textsuperscript{50}
\end{quote}

Section 230 absolves providers, like Facebook and Twitter, from liability for the content on their platform and for any moderation of that content conducted in good faith.

The United States commitment to free speech has not only stymied attempts at domestic regulation,\textsuperscript{51} but it has undermined European efforts to construct a regulatory system for hate speech.\textsuperscript{52} In 2000, the \textit{International League against Racism and Anti-Semitism}, a French organization, challenged \textit{Yahoo!} in U.S. courts to stop the online sale of Nazi memorabilia to French citizens, a crime under French hate speech laws. The courts ruled that online sales made by a U.S. company whose servers reside in the United States were protected under the first amendment.\textsuperscript{53} While the courts have upheld freedom of speech protections, they have struggled to define what exactly constitutes protected speech,\textsuperscript{54} and they are nowhere near establishing a litmus test for information that could be considered extreme, illicit, or damaging.

Policy issues aside, it is possible that no amount of legislation can improve the information environment. In 2017, the Pew Research Center released \textit{The Future of Truth and Misinformation Online} report which surveyed over 1,100 experts to see what the next 10 years of combating fake news and online misinformation will look like.\textsuperscript{55} Experts were almost perfectly split in their opinion as to whether the information environment would improve.\textsuperscript{56} Experts that believed the environment would not improve generally cited two reasons:
The fake news ecosystem preys on some of our deepest human instincts: Respondents said humans’ primal quest for success and power – their "survival" instinct – will continue to degrade the online information environment in the next decade. They predicted that manipulative actors will use new digital tools to take advantage of humans’ inbred preference for comfort and convenience and their craving for the answers they find in reinforcing echo chambers.

Our brains are not wired to contend with the pace of technological change: These respondents said the rising speed, reach and efficiencies of the internet and emerging online applications will magnify these human tendencies and that technology-based solutions will not be able to overcome them. They predicted a future information landscape in which fake information crowds out reliable information. Some even foresaw a world in which widespread information scams and mass manipulation cause broad swaths of public to simply give up on being informed participants in civic life.57

The more optimistic half of those experts surveyed inverted this reasoning:

Technology can help fix these problems: These more hopeful experts said the rising speed, reach and efficiencies of the internet, apps and platforms can be harnessed to rein in fake news and misinformation campaigns. Some predicted better methods will arise to create and promote trusted, fact-based news sources.

It is human nature to come together and fix problems: The hopeful experts in this canvassing took the view that people have always adapted to change and that this current wave of challenges will also be overcome. They noted that misinformation and bad actors have always existed but have eventually been marginalized by smart people and processes. They expect well-meaning actors will work together to find ways to enhance the information environment. They also believe better information literacy among citizens will enable people to judge the veracity of material content and eventually raise the tone of discourse.

Perhaps decision makers will eventually succeed in finding an effective policy that balances freedom of speech with safety from weaponized information. Until then, social media platforms will continue to police themselves.58

Endnotes

5 Ibid.


14 Ibid.

15 House Intelligence Committee, Exposing Russia’s Effort to Sow Discord Online: The Internet Research Agency and Advertisements.


20 Ibid.


22 Giles, Handbook of Russian information warfare.

23 Ibid.

24 Ibid.


26 Ibid.

27 Andrew Weisburd, Clint Watts, and J.M. Berger, Trolling for Trump: How Russia Is Trying to Destroy Our Democracy.


30 Giles, Handbook of Russian information warfare.

31 Helmus et al., Russian social media influence: Understanding Russian propaganda in Eastern Europe.


34 Ibid.

35 Helmus et al., *Russian social media influence: Understanding Russian propaganda in Eastern Europe*.


41 Ibid.


43 Jana Winter, *Exclusive: FBI document warns conspiracy theories are a new domestic terrorism threat*.

44 Ibid.


47 Cook, “YouTube’s Plan To Rein In Conspiracy Theories Is Failing”.


53 Ibid.


56 Ibid.

57 Ibid.

58 Brannon, “Free Speech and the Regulation of Social Media Content”.
**Recommended Reading**


