EC-130J Commando Solo systems operator monitors broadcast during mission in support of Operation *Inherent Resolve* at undisclosed location in Southwest Asia, September 5, 2017 (U.S. Air Force/Michael Battles)

What's Not to Like?

Social Media as Information Operations Force Multiplier

By Glenda Jakubowski

In June 2013, Vladimir Putin stated that Russia must "break the Anglo-Saxon monopoly on global information streams."[1] By April 2014, Russia's Internet Research Agency (IRA) formed the "translator project," which "focused on the U.S. population and conducted operations on social media platforms such as YouTube, Facebook, Instagram, and Twitter."[2] Four years after the translator project began operations, Special Counsel Robert Mueller issued an indictment against three Russian companies and 13 Russian individuals, alleging Russian actors stole the identities of individual Americans, posed as individual Americans, posed as American interest groups and political activists, hacked voter registration data, and scraped social media profiles to influence U.S. elections and political processes. The information operations would be "the most effective and efficient influence campaign in world history," according to Clint Watts, a senior fellow in the Center for

Glenda Jakubowski is an Intelligence Analyst at the Defense Intelligence Agency.

Cyber and Homeland Security at The George Washington University.[3] It was social media that made Russia's information operations so effective and efficient, particularly social media–enabled social engineering, identity theft, targeted advertisements, profiling through psychometrics, dissemination through bots, trending algorithms, creation of false personas, and psychological hacks to increase trust and verisimilitude. The psychology behind pleasure, rewards, social groups, and fear makes social media addictive and credible. This is the same psychology that makes social media's use in information operations so pernicious and possibly impossible to counter.

Russia has used social media to foster conspiracy theories, plant rumors, and spread fake news in Bulgaria, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Serbia, Spain, Sweden, Ukraine, the United Kingdom, and the United States.[4] Experts have correlated Russian information operations with the referendums on Brexit, Scottish independence, and Catalonian secession from Spain, and in one academic study, researchers correlated Russian information operations with changes in U.S. voter behavior that possibly affected the outcome of the 2016 Presidential election.[5]

Russia's information operations successes, however, are not uniform. Factors that contributed to or mitigated Russian information operations successes include the target nations' historical relationships with Russia, percentage of ethnic Russians in the population, ethnic homogeneity, racial conflict, migration, national control of media and the Internet, and the level of trust between citizens and their governments. Many of these factors make the United States, with its constitutional freedoms, Internet saturation, and political and racial divides, particularly vulnerable to and less able to defend against these information operations.

Social Media Is a Game Changer

According to testimony by Clint Watts before the U.S. Senate Committee on the Judiciary, five social media functions are necessary for "full-spectrum social media campaigns: reconnaissance, hosting, placement, propagation, and saturation."[6] Russia used all of these in its information operations against the West. Briefly, *reconnaissance* in social media equates to knowing the target audience, and *hosting* refers to the site, such as YouTube, Facebook, or Twitter. *Placement*, during the Cold War, referred to placing forged items in news outlets that unknowingly published the items as authentic. In current usage, it is placing "digital forgeries" on sites such as 4chan and Reddit that then spread to mainstream sites, fueling conspiracy theories and false narratives. *Propagation* refers to spreading narratives broadly and quickly, which social media particularly enables through such means as bots that cause news items to trend, increasing the likelihood they will jump to mainstream media. Finally, the networked nature of social media enables *saturation* in multiple types of media outlets, which lends credibility to false stories. According to Watts, Russia is the first entity to incorporate the "entire social media ecosystem" into its information operations.[7]

The Social Media Ecosystem

The combination of false news, social media, politics, conspiracy theories, sensationalism—and human nature—creates a perfect propaganda storm. Studying 126,000 news stories shared from Twitter's inception in 2006 until 2017 by approximately 3 million people, researchers found that false news spreads "further, faster, deeper, and more broadly" than legitimate news—even more so for false news about political subjects compared to items about "terrorism, natural disasters, science, urban legends, or financial information."[8] The researchers found that bots speed the dissemination of true and false stories equally; although bots may increase the amount of information spread through social media, it is humans that spread false news more quickly than factual news. Thus, false tweets reached more people than true tweets; true tweets rarely reached as many as 1,000 people, compared to false tweets, which routinely reached up to 100,000 people. Additionally, false information spread six times faster than true information, and false political information spread even more quickly and was more viral.[9]

The data scraping enabled by firms such as Cambridge Analytica is an example of reconnaissance. Cambridge Analytica brought "big data and social media to an established military methodology—information operations—then turn[ed] it on the U.S. electorate."[10] The company analyzed potential voters' social media profiles, then sent the users "micro-targeted" Facebook advertisements to influence their voting behavior. In 2017, the Cambridge Analytica chief executive officer (CEO) boasted at a marketing conference that he had about 5,000 separate bits of information on each of 220 million Americans and that his company had "played a significant role" in contributing to the success of the Presidential campaign. Cambridge Analytica applied analysis to these discrete bits of information gleaned from Facebook profiles and from publicly available information to "send the right people to the right ads through cookie matching, mail shots, set-top box viewing data matching, and highly targeted, non-public, paid Facebook posts often referred to as 'dark ads.'"[11]

In 2014, Cambridge Analytica presented slides on how to disrupt elections to a Russian oligarch with strong ties to Vladimir Putin, ostensibly to solicit oil contracts.[12] Coincidentally, Russia around this time began to use micro-targeting in social media to attempt to influence the 2016 U.S. Presidential election.[13] In U.S. Senate committee hearings in 2018, when asked whether the 126 million users the Russian IRA targeted with Facebook ads were also among those whose data Cambridge Analytica accessed, Facebook CEO Mark Zuckerberg replied, "We believe it is entirely possible."[14]

Whether or not Russia directly used data gained from Cambridge Analytica, by 2015 Russia was using social media to spread conspiracy theories to specific

audiences surrounding issues that would become 2016 campaign hot buttons, including gun rights, big government, and Islamophobia. One of its targets, according to former Central Intelligence Agency director Michael Hayden, was a 2015 U.S. military exercise conducted in seven southern U.S. states called Jade Helm 15.[15]

Jade Helm 15 was a U.S. Special Operations Command joint exercise conducted in Texas, New Mexico, Arizona, California, Nevada, Utah, and Colorado from July 15 to September 15, 2015, to improve special operations forces' unconventional warfare capabilities.[16] However, conspiracies propagated on Russia-controlled Instagram, Twitter, and YouTube accounts and Russia-created Facebook pages, such as Heart of Texas, claimed Jade Helm 15 variously was a psychological operation to build complacency about the military's presence in the affected states to enable an eventual invasion, an international or United Nations (UN) operation to seize citizens' guns, a military operation to round up political dissidents, a military operation to remove state and local political leaders who would oppose the Federal Government's imposition of martial law, an operation using recently closed Walmarts to supply invading Chinese troops, or a military plan to impose martial law and disarm citizens in the wake of an apocalyptic meteor strike predicted to occur the same day Jade Helm 15 concluded.[17] As bizarre as they seem, the conspiracies surrounding Jade Helm 15 garnered reactions from U.S. politicians—reactions that gave credence to the Russian information operations. These included Texas governor Greg Abbott calling on the Texas State Guard (equivalent to the National Guard) to monitor the exercise, Senator Rand Paul (R-KY) promising to "look into" the exercise, Senator Ted Cruz (R-TX) assuring constituents that he had inquired about the exercise from Pentagon officials "because the Federal Government has not demonstrated itself to be trustworthy," and Representative Louie Gohmert (R-TX) demanding the military revamp the exercise "so the Federal Government is not intentionally practicing war against its own states."[18] The Jade Helm 15 information operation is an example of hosting, placement, propagation, and saturation.

Russia's social media–enabled information operations continue to garner official responses, which give the impression that Russia's false news is authentic. According to an NBC News report, more than 40 celebrities and politicians were "roped into retweeting or otherwise engaging with accounts created by a Russian 'troll factory' to millions of followers," and 3,000 news outlets worldwide published articles containing embedded Russian troll farm tweets in the runup to the 2016 election—an example of stunningly successful placement.[19] Cross-referencing a list of IRA Twitter handles with archived tweets by nearly 900 politicians and celebrities, NBC found the list of influential people who have retweeted or engaged with Russian propagandists includes President Donald Trump; his son, Donald Trump, Jr.; white nationalist Richard Spencer; Trump political associate Roger Stone; former UN Ambassador Samantha Power; former Ku Klux Klan grand wizard David Duke; Senator John Coryn (R-TX); Kellyanne Conway; Women's March coordinator Linda Sarsour; Michael Flynn, Jr.; Ohio senator Nina Turner; Ted Cruz; former White House communications director Anthony Scaramucci; former White House press secretary Sean Spicer; Sean Hannity; Ann Coulter; Laura Ingraham; Jake Tapper; Lou Dobbs; Nikki Minaj; Sarah Silverman; Trevor Noah; the *Washington Post*; *Breitbart*; *Buzzfeed*; the *Daily Mail*; UN officials; academics; and authors from both the right and left.[20] Celebrity retweeters who agree with the original tweets add credibility to the Russian propaganda. But even when celebrities disagree with the original sentiment, their celebrity status aids in the propaganda dissemination through the social media phenomenon of trending.

Social media groups tend to share worldviews, in a phenomenon called *homophily*.[21] Homophily and data scraping enabled Russia to target social media network groups most likely to believe the information operations message and most likely to share it with similarly minded groups. In this manner, a false news item can metastasize quickly from a small number of discrete cells to a trending conspiratorial cancer in a matter of days or hours. The Comet Ping Pong conspiracy provides an example.

The information operation involving the "news" that Hillary Clinton and other Democrats were pedophiles running a sex ring out of a restaurant, Comet Ping Pong, in Washington, DC, almost certainly began with the Russian military intelligence service hack of John Podesta's email server on March 19, 2016. Among those emails were exchanges between Podesta and his friend, Comet Ping Pong owner James Alefantis.[22] WikiLeaks published the hacked emails on October 7, 2016, and by late October, the first allegations about Comet Ping Pong appeared in a few posts on 4chan and another anonymous message board that purported to cater to New York Police Department (NYPD) users. Within hours of the putative NYPD post, a real person posted about the alleged sex ring on Facebook, citing her "NYPD source." Four days later, the conspiracy theory–themed show, *Info Wars*, broadcasted the story. The conspiracy also was mentioned on a law enforcement Facebook page, and from there a Russian bot posing as a U.S. Air Force veteran posted it on Twitter. The bot, whose profile picture shows a middle-aged woman, has followers that include former Trump deputy assistant Sebastian Gorka and former National Security Adviser Michael Flynn. Eventually, the Comet Ping Pong conspiracy would be shared 1.4 million times, including by at least 14 Russian bots and by real people including Donald Trump, Jr.; Paul Manafort; Ann Coulter; and Roger Stone. On December 4, 2016, a North Carolina man fired an AR-15 rifle in the occupied Comet Ping Pong restaurant, seeking to free the children he thought were held there as sex slaves for the Clintons and their friends.[23] As of June 2018, a cursory search revealed multiple current social media posts on YouTube, Twitter, and Facebook claiming "Pizzagate" is real and that the Clintons

Comet Ping Pong façade in Washington, DC, December 11, 2016 (Courtesy Farragutful)

and Democrats are continuing to run pedophile and human-trafficking rings.

Why would Russia promote conspiracy theories as part of its information operations? Russia scholar Ilya Yablokov asserts it is because the conspiracy theories are "a specific tool of Russian public diplomacy aimed at undermining the policies of the U.S. Government."[24] Crucially, the conspiracy theories—and the information operations—are not challenges to ideology; Russia's information operations today are not a reprise of Soviet-era communism-versus-capitalism battles for hearts and minds. The current goal for Russia is to "undermine trust in information generally."[25] Among the ways to do so is to use specific, trustworthy messengers, which is where Russia's use of stolen social media profiles and micro-targeted outreach come in.

In early June 2016, the Web site DCLeaks went live, featuring stolen emails from the Democratic National Committee. Eventually DCLeaks would post emails stolen from more than 300 high-ranking government and military officials. The U.S. Intelligence Community assesses DCLeaks to be linked to Russian military intelligence and the Russian hacking entity Guccifer 2.0.[26] Within days of DCLeaks's launch, "Melvin Redick," allegedly of Harrisburg, PA, posted a link to DCLeaks on multiple Facebook group pages.[27] Melvin Redick, however, does not exist. He is a fake persona created by Russian actors using the stolen Facebook profile of a Brazilian salesman.[28] Similar posts by "Alice Donovan" and "Katherine Fulton" appeared on Facebook the same day.[29] As with Melvin Redick, Alice Donovan and Katherine Fulton are fake personas created by Russian cyber actors. Their posts targeted real Facebook users who Russian cyber actors determined, through psychometric profiling such as that done by Cambridge Analytica, would be most susceptible to their messages. In concert with the Facebook posts, hundreds of Twitter posts also linked to DCLeaks, Guccifer 2.0, or similar sites associated with Russian intelligence. Many of these were fueled by bots, some hijacked legitimate Twitter accounts, and many included the Twitter handles of mainstream news organizations or influential accounts, including @realDonaldTrump.[30] These events are examples of reconnaissance, hosting, placement, propagation, and saturation.

A Florida voter was one of the people Russia selected as part of its

Soldiers from Bronco 71 Team, operating with members of civil affairs, psychological operations, and information operations trainers, tie M240B machine gun to saddle during mule packing training, August 1, 2017, Fort Irwin, California (U.S. Army/Austin Anyzeski)

micro-targeting reconnaissance efforts. In August 2016, a stranger sent her a private message on Facebook from a Russia-affiliated fake Facebook group called Being Patriotic, asking her to organize a pro-Trump rally. The Russians chose well in targeting this woman, who showed up for the rally dressed as Hillary Clinton in a prison jumpsuit.[31] In addition to that person (who was not paid), Russia used micro-targeting to pay multiple Floridians to build cages and pose as Clinton behind bars.[32] Another person, also from Florida, responded to a Being Patriotic Facebook request that he host a pro-Trump gathering.[33] Similarly, another Floridian agreed to wave pro-Trump signs at a rally after receiving a phone call in August 2016 from a stranger from a Russian front group called Florida Goes Trump.[34] Yet another Floridian received a phone call out of the blue, followed by emails from people she thought to be college students from Texas but who actually were Russians.[35] She received about $600 and a script from the Russians to don a Hillary Clinton mask and an orange jail jumpsuit to participate in one of 20 pro-Trump rallies in Florida scheduled for the same day in August. And still another individual received a similar payment after Russians posing as Americans contacted him on the Being Patriotic Facebook page, asking him to build a cage as part of the same rally.[36]

None of the targeted Americans, when informed of the Russian origins of the requests for political activity, considered the Russian interference a problem. They dismissed concerns over the Russian effort as a "waste of time," insisted they would have held rallies for Trump or parodied Clinton anyway without Russian trickery, and claimed the Russian efforts had no effect because the targeted voters "didn't need persuading."[37]

Many of the examples above demonstrate the psychological aspects of social media that make it so effective as a force multiplier in information operations. They show Russia's use of psychological factors such as homophily, or retweets by trusted or influential people, or receiving phone calls, emails, and private messages from "friends," to pressure its adversaries to accept false stories as truthful. In addition to these, Russia also exploits the fact that social media itself has been designed to activate areas in the brain associated with rewards and addiction.

According to neuroscientist Shannon Odell, people use social media such as Facebook and Twitter for two reasons: to connect with people and to control the impressions they make on others. The "like," "share," or "retweet" is positive reinforcement for both of those motivators, activating neural pathways for reward and addiction.[38] Additionally, when users in one experiment were shown photographs, the photographs with more "likes" activated the brain's reward

circuitry more than the photographs with fewer "likes." People are apt to approve of social media posts their friends approve of, even if those "friends" are strangers.[39] Yet another study corroborates the power of the "like," finding that social media users are more likely to adopt those emotions that are "over-expressed in their social network."[40] The level of emotional "contagion" is significantly influenced when the agent seeking to spread an idea uses bots. Russian information operations benefited from not only the mechanics of bot propagation and troll farm employees generating multiple "likes" and "shares" to influence trends algorithms, but also the psychological tendencies of humans exposed to bot propagation and to "peer group" emotions. A user confronted with false news on social media that comes appended with hundreds of bot-generated "likes" is psychologically apt to believe and spread the false news.

Among the most pervasive questions regarding social media and false news in the 2016 U.S. election is did they make a difference in the final vote tally. A definitive answer is difficult. However, according to one scholarly study and *Washington Post* analysis, the data correlate with an affirmative response. Using multiple regression analyses, Ohio State University researchers concluded that believing false news encountered on social media was among the top four variables predicting that a voter who previously supported Barack Obama would "defect from the Democratic ticket in 2016." Respondents to an Ohio State survey who believed at least one false news item plucked from social media were 4.5 times more likely to have voted against Clinton than respondents who believed none of the false news items in the survey.[41] Using the Ohio State data in predictive probability analysis, the *Washington Post* polling director assessed that false news likely cost Clinton 4.2 percent of votes overall and approximately 2.2 percentage points in the battleground states of Michigan, Pennsylvania, and Wisconsin. In the 2016 election, Clinton lost Michigan by 0.2 percentage points, Pennsylvania by 0.72 percentage points, and Wisconsin by 0.76 percentage points.[42]

Europe's Answer to Russian Information Operations

Finland is the commonly cited example of how to counter Russia's information operations. Finland's tactics include a public diplomacy program with support from the Finnish president, who declared it the responsibility of every citizen to combat Russian information operations, and support from the prime minister's office, which enrolled hundreds of government officials in programs to understand how disinformation spreads. Experts also credit Finland's public education system—which ranks top in the world—with building critical thinking skills that help strengthen Finns against disinformation. Additionally, Finns have a high level of trust in their government and a high level of distrust for Moscow. Finland also has demographics to thank for its ability to fend off Russian propaganda; the Finnish population of 5.5 million is quite homogeneous, with a minimal number of Russian speakers.[43] Only 3.5 percent of people living in Finland are foreign born, one of the lowest rates in the European Union (EU), and the Russian population in Finland is 0.5 percent, compared to 93 percent native Finns.[44] Finns are more alike than they are different from one another, which makes it difficult for information campaigns focused on exploiting social rifts to take hold.

Other Baltic nations, such as Latvia, Lithuania, and Estonia, have been less successful against Russian information operations. These nations have larger numbers of Russian speakers among their populations and the strong presence of the Russian-language, Russia-owned television station, Channel One. In Finland, the Russia-owned, Russian-language Sputnik television station lacked enough viewers to remain operational; in Latvia, Lithuania, and Estonia, government moves to block Russian programming backfired, leading to protests from the Russian populations in those countries and feeding the Russian propaganda narrative of marginalization.[45] The Baltic states do focus on countering Russian propaganda, but "if you only focus on countering, you're on their territory," stated a member of the Strategic Communications Center of Excellence in Latvia.[46] Finland is an outlier, then, and it seems unfair to suggest others use it as a model, when the variable that likely works most toward Finland's favor—its homogeneity—is outside other nations' control. Other European countries have been tackling the Russian information operations problem, including, in some cases, the social media aspect of the operations. Some examples follow:

- **Tracking False News**
  - Britain, France, Germany, the Czech Republic, the Netherlands, Switzerland, Finland, Sweden, Ukraine, Latvia, and Slovakia maintain sites to track false news and social media conspiracy theories.[47]
  - The EU's EAST Stratcom Task Force publishes a weekly disinformation review in 18 languages—including calling out fake fact-checkers that appear to be the work of Russia.[48]
- **Working with Media, Social Media, and Advertisers**
  - More than 1,400 advertisers in Slovakia are boycotting a list of false Web sites compiled by a nonprofit researcher.[49]
  - The night before the French presidential election, Russian military intelligence hackers released hacked emails and documents connected to then-candidate Emmanuel Macron. Most French media outlets agreed to election commission requests to refrain from publishing the hacked documents.[50]
  - Facebook agreed to requests from France and Britain to disable multiple thousands of false accounts connected to elections.[51]
  - Sweden urges all mainstream media to fact-check news stories.[52] Mainstream media, of course, is not the major purveyor of false stories, and Sweden so far is doing nothing about the Russian

U.S. psychological operations Soldiers with Combined Joint Special Operations Task Force–Iraq conduct radio-in-a-box training with members of Iraqi Counter-Terrorism Service psychological operations team, in Baghdad, February 10, 2019 (U.S. Army/Sarah K. Anwar)

trolls that are averaging 2,000 comments per person, per inflammatory news item posted on a right-wing site.[53]

- **Legal Measures**
  - The French electoral code makes it illegal to "broadcast to the public by any means of electronic communication anything that could be considered electoral propaganda."[54]
  - The EU has enacted a code of practice against disinformation aimed at social media companies that requires them to prevent "disinformation and the manipulative use of platforms' infrastructure."[55]
  - On May 25, 2018, the EU enacted the General Data Protection Regulation (GDPR), which applies to all companies doing business in the EU regardless of the companies' locations. The GDPR guarantees EU citizens the right to know of data breaches within 72 hours, the right to access their data from social media companies and to know where and for what purpose their data is used, the "right to be forgotten," the right to data portability, and the right to privacy by design—that is, the inclusion of data protection from the onset of designing systems. Failure to abide by the GDPR can result in tiered fines of up to 4 percent of profits or 20 million euros.[56]
- **Political Cooperation.** German political parties agree not to use bots in their social media campaigns. (Russia continues to use bots on social media in Germany, however.)[57]
- **Public Diplomacy.** Sweden distributes pamphlets advising Swedes what to do in case of war with Russia, or terrorist attacks, in an attempt to shape how Swedish citizens think about Russia.[58]
- **Countermessaging**
  - The United Kingdom, Germany, Latvia, Lithuania, and Estonia are countermessaging Russia Today and Sputnik "news" items.[59]
  - Also, in Lithuania, citizen volunteers who call themselves elves "identify and beat back the 'trolls' employed on social media to spread Russian disinformation."[60]
- **Government Initiatives.** In Sweden, the Swedish Civil Contingencies Agency, which is roughly equivalent to the U.S. Department of Homeland Security, monitors Web sites for false, inflammatory stories.[61]

What About the United States?

The United States shares some challenges with its European partners in fighting Russian information operations and also has some U.S.-specific challenges. The United States is far from homogeneous; according to the Census Bureau in 2017, about 60.7 percent of

Civilian role players help 80th Training Command's psychological operations students learn to negotiate difficult terrain of cultural, social, and political differences during training exercise at Fort Hunter Liggett, California, February 6, 2019 (U.S. Army/Cynthia McIntyre)

the population is white, 18.1 percent is Hispanic (which can be any race), 13.4 percent is black, 5.8 percent is Asian, 2.7 percent are mixed race, and 1.5 percent are other.[62] Russia laser-targeted racial and social divides in America during the runup to the 2016 election, as well as controversies over immigration, gun control, Islamophobia, gay rights, and other divisive topics. Russia continues, post-election, to use social media in information operations to "create general distrust or confusion about information sources by blurring the lines between fact and fiction."[63]

The United States is unlikely to enact a domestic propaganda program such as Finland's. Reforms of the Smith-Mundt Act in 2013 allow domestic broadcasts of State Department programming produced for foreign audiences, such as Voice of America broadcasts, but forbid broadcasting propaganda *targeting* American audiences.[64] However, reactions from some politicians and defense officials to the reforms indicate the suspicion many in the United States feel toward government information programs. Opponents claimed the reforms would make Americans vulnerable to government disinformation campaigns to "prop up unpopular policies" and "remove protections" against U.S. Government information campaigns targeting U.S. citizens that may be "inaccurate or completely false."[65] That the opponents were themselves presenting inaccurate information about the new Smith-Mundt Act did little to reduce confusion surrounding the reforms, but much to illuminate the distrust many Americans likely would feel toward a domestic government information campaign.

After Facebook CEO Mark Zuckerberg's House and Senate testimony on Cambridge Analytica's breach of users' data, Senator Amy Klobuchar (D-MN) and Senator John Kennedy (R-LA) introduced the Social Media Privacy Protection and Consumer Rights Act, which is similar to the GDPR. The bill requires social media companies to disclose to users what data are being collected on them, who has access to user data, and how companies that have that access are using the data. The bill also allows users to opt out of having their data collected and to demand that Web sites delete any data that had been collected on them.[66] As of this writing, the proposal has been sitting in the Commerce, Science, and Transportation Committee since late April 2018.[67]

Conclusion: A Social Media Problem Requires a Social Media Solution

Measures such as the Code of Practice on Disinformation, GDPR, and Social Media Privacy Protection and Consumer Rights Act will mitigate social media–enabled information operations because they empower privacy and data protection. However, these measures will not eliminate the psychological aspects of social media that make it such a powerful tool for information operations. Humans are motivated by

desire and fear. Just as "likes" activate areas of the brain associated with desire, conspiracy theories and false news about other races, other religions, and other opinions activate fears in susceptible audiences. What makes the United States strong—its technology, its diversity, its commitment to free speech—also, unfortunately, makes it enduringly vulnerable to information operations by an adversary such as Russia.

The Constitution prohibits the U.S. Government from restricting free speech. But private companies are free to set their own limits, and indeed, social media companies such as Facebook have removed hundreds of fake accounts since the hearings looking into Russia's use of social media in its information operations. Public scrutiny can pressure private companies to prohibit data mining and practice due diligence against foreign entities using their platforms against the United States. The United States can mitigate—somewhat—social media–enabled information operations. But governments cannot mitigate neuropsychology. No amount of critical thinking education, anti-Russia pamphleteering, domestic propaganda, or "outing" Russia (recall the Americans duped by Russians who, after learning the truth, stated they were unconcerned about being Russian targets) will eliminate the neural feedback loop that is reinforced every time users are deceived by hundreds of artificially placed "likes" or retweets. Humans are wired to believe. **JFQ**

Notes

[1] Jill Dougherty, "How the Media Became One of Putin's Most Powerful Weapons," *The Atlantic Monthly*, April 21, 2015, available at <www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/>.

[2] *United States v. Internet Research Agency et al.*, Case 1:18-cr-00032-DLF, February 16, 2018, available at <www.justice.gov/file/1035477/download>.

[3] Clint Watts, "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014," *The Daily Beast*, March 30, 2017, available at <www.thedailybeast.com/clint-watts-testimony-russias-info-war-on-the-us-started-in-2014>.

[4] U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," S. Prt. 115-21, 115th Cong., 2nd sess., 2018, available at <www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>.

[5] Ibid.; Richard Gunther, Paul A. Beck, and Erik C. Nisbet, "Fake News May Have Contributed to Trump's 2016 Victory," Ohio State University, March 8, 2018, available at <www.documentcloud.org/documents/4429952-False-News-May-Have-Contributed-to-Trump-s-2016.html>.

[6] Clint Watts, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," Judiciary Subcommittee on Crime and Terrorism questions for the record, October 31, 2017, and hearing, November 7, 2017, available at <www.judiciary.senate.gov/imo/media/doc/Watts%20Responses%20to%20QFRs.pdf>.

[7] Ibid.

[8] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018), 1146–1151, available at <http://science.sciencemag.org/content/359/6380/1146.full>.

[9] Ibid.

[10] Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," *The Guardian*, March 18, 2018, available at <www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.

[11] Charles Kriel, "Fake News, Fake Wars, Fake Worlds," *Defence Strategic Communications* 3 (Autumn 2017), 172–190.

[12] Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool.'"

[13] *United States v. Internet Research Agency et al.*

[14] "Transcript of Mark Zuckerberg's Senate Hearing," *Washington Post,* April 10, 2018, available at <www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.ce270a6edca3>.

[15] Cassandra Pollock and Alex Samuels, "Hysteria Over Jade Helm Exercise in Texas Was Fueled by Russians, Former CIA Director Says," *Texas Tribune*, May 3, 2018, available at <www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/>.

[16] U.S. Army Special Operations Command, "Request to Conduct Realistic Military Training (RMT) JADE HELM 15," 2015, available at <https://docs.google.com/file/d/0B3axduuybL0jdjZQUjhsSmJsZTA/edit>.

[17] Jim Shea, "Thank You Texas and Good Luck with the Invasion," *Hartford Courant*, May 17, 2015, available at <www.courant.com/features/too-shea/hc-shea-weekinreview-0517-20150517-column.html>; Jon Austin, "U.S. Military Secretly Planning for Giant Asteroid That Will Wipe Out Mankind in September," *Daily Express* (London), June 8, 2015, available at <www.express.co.uk/news/weird/583002/US-military-secretly-preparing-asteroid-wipe-out-mankind-September-Jade-Helm>.

[18] Pollock and Samuels, "Hysteria Over Jade Helm Exercise in Texas Was Fueled by Russians." Patrick Svitek, "Jade Helm 15: The Black Helicopters Are Coming. Well, Maybe Not," *Texas Tribune*, April 30, 2015, available at <www.texastribune.org/2015/04/30/abbotts-letter-puts-jade-helm-national-stage/>; David Weigel, "Ted Cruz Says He Has Asked the Pentagon for Answers on Jade Helm 15," *Bloomberg*, May 2, 2015, available at <www.bloomberg.com/news/articles/2015-05-02/ted-cruz-says-he-has-asked-the-pentagon-for-answers-on-jade-helm-15>; Louie Gohmert, "Gohmert Statement on Jade Helm Exercises," May 5, 2015, available at <https://gohmert.house.gov/news/documentsingle.aspx?DocumentID=398216>.

[19] Ben Popken, "Russian Trolls Duped Global Media and Nearly 40 Celebrities," NBC News, November 3, 2017, available at <www.nbcnews.com/tech/social-media/trump- other-politicians-celebs-shared-boosted-russian-troll-tweets-n817036>.

[20] Ibid.

[21] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017), 50–85.

[22] Cecilia Kang, "Fake News Onslaught Targets Pizzeria as Nest of Child-Trafficking," *New York Times*, November 21, 2016, available at <www.nytimes.com/2016/11/21/technology/fact-check-this-pizzeria-is-not-a-child-trafficking-site.html>.

[23] Amanda Robb, "Anatomy of a Fake News Scandal," *Rolling Stone*, November 16, 2017, available at <www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877/>.

[24] Ilya Yablokov, "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)," *Politics* 35, no. 3/4 (2015), 301–315.

[25] Kate Starbird, "Information Wars: A Window into the Alternative Media Ecosystem," HCI and Design at UW, March 14, 2017, available at <medium.com/hci-design-at-uw/information- wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f>.

[26] "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections': The Analytic Process and Cyber Incident Attribution," ICA 2017-01D (Washington, DC: Office of the Director of National Intelligence, January 6, 2017), available at <www.dni.gov/files/documents/ICA_2017_01.pdf>.

[27] Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017, available at <www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html>.

[28] Scott Shane, "Mystery of Russian Fake on Facebook Solved, by a Brazilian," *New York Times*, September 13, 2017, available at <www.nytimes.com/2017/09/13/us/politics/russia-facebook-election.html>.

[29] Shane, "The Fake Americans Russia Created to Influence the Election."

[30] Ibid.

[31] Anton Troianovski et al., "The 21st-Century Russian Sleeper Agent Is a Troll with an American Accent," *Washington Post*, February 17, 2018, available at <www.washingtonpost.com/business/technology/the-21st-century-russian-sleeper-agent-is-a-troll-with-an-american-accent/2018/02/17/d024ead2-1404-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.aa5c01a98cfa>.

[32] *United States v. Internet Research Agency et al.*

[33] Troianovski et al., "The 21st-Century Russian Sleeper Agent Is a Troll with an American Accent."

[34] Ashley Parker and John Wagner, "'Go Donald!': Inside the Russian Shadow Campaign to Elect Trump," *Washington Post*, February 16, 2018, available at <www.washingtonpost.com/politics/go-donald-inside-the-russian-shadow-campaign-to-elect-trump/2018/02/16/dea562c2-134a-11e8-9065-e55346f6de81_story.html?utm_term=.a1ce4565b4bd>.

[35] Frank Cerabino, "Local Trump Supporters Shrug Off Being Paid and Played by Russians," *Palm Beach Post*, February 23, 2018, available at <www.palmbeachpost.com/news/local-trump-supporters-shrug-off-being-paid-and-played-russians/3WCytHAHy3PodLVePU1PMK/>.

[36] Ibid.

[37] Parker and Wagner, "'Go Donald!'"; Troianovski et al., "The 21st-Century Russian Sleeper Agent Is a Troll with an American Accent."

[38] Shannon Odell, "Your Brain on Social Media: Neuroscientist Shannon Odell Explores the Insatiable Effects and Drivers of Social Media Addiction," *PR Newswire*, April 24, 2018.

[39] "Social Media 'Likes' as Yummy as Chocolate," *Science Teacher* 83, no. 6 (2016), 20–22.

[40] Emilio Ferrara and Zeyao Yang, "Measuring Emotional Contagion in Social Media," *PLOS ONE* 10, no. 10 (2015), 1–14, available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0142390>.

[41] Gunther, Beck, and Nisbet, "False News May Have Contributed to Trump's 2016 Victory."

[42] Aaron Blake, "A New Study Suggests False News Might Have Won Donald Trump the 2016 Election," *Washington Post*, April 3, 2018, available at <www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/?utm_term=.ddaa357e0020>.

[43] Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*, March 1, 2017, available at <http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/>.

[44] See "Finland Population 2019," World Population Review, available at <http://worldpopulationreview.com/countries/finland-population/>; and "Finland Demographics Profile 2018," Index Mundi/CIA World Factbook, available at <www.indexmundi.com/finland/demographics_profile.html>.

[45] Standish, "Why Is Finland Able to Fend Off Putin's Information War?"

[46] Christian Caryl, "If You Want to See Russian Information Warfare at Its Worst, Visit These Countries," *Washington Post*, April 5, 2017, available at <www.washingtonpost.com/news/democracy-post/wp/2017/04/05/if-you-want-to-see-russian-information-warfare-at-its-worst-visit-these-countries/?utm_term=.1ab2a9e9a132>.

[47] Dana Priest and Michael Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years," *Washington Post*, June 25, 2017, available at <www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42d-cece-4a09-11e7-9669-250d0b15f83b_story.html?utm_term=.8c9dd9d96071>.

[48] "Behind the Scenes at the Swedish Troll Factory," EU vs. Disinformation Campaign, February 20, 2017, available at <https://euvsdisinfo.eu/behind-the-scenes-at-the-swedish-troll-factory/>.

[49] Priest and Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years."

[50] Alex Hern, "Macron Hackers Linked to Russian-Affiliated Group Behind U.S. Attack," *The Guardian*, May 8, 2017, available at <www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack>; Priest and Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years."

[51] Priest and Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years."

[52] Michael Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections. The White House Might Take Note," *Washington Post*, February 22, 2018, available at <www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html?utm_term=.b871124aed50>.

[53] "Behind the Scenes at the Swedish Troll Factory."

[54] Kim Willsher and Jon Henley, "Emmanuel Macron's Campaign Hacked on Eve of French Election," *The Guardian*, May 6, 2017, available at <www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>.

[55] Julia Fioretti, "EU Piles Pressure on Social Media Over Fake News," Reuters, April 26, 2018, available at <www.reuters.com/article/us-eu-internet-fakenews/eu-piles-pressure-on- social-media-over-fake-news-idUSKBN1HX15D>.

[56] General Data Protection Regulation portal, available at <www.eugdpr.org>.

[57] Priest and Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years."

[58] Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections."

[59] Caryl, "If You Want to See Russian Information Warfare at Its Worst, Visit These Countries."

[60] Priest and Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years."

[61] Ibid.

[62] U.S. Census Bureau Quick Facts, 2017, available at <www.census.gov/quickfacts/fact/table/US/PST045217>. These percentages add to 102.2 percent. To reach the correct 100 percent, one has to subtract those who identified as "White alone" (76.6 percent) from those who identified as "White alone, not Hispanic or Latino" (60.7 percent). The resulting difference has to be subtracted from those who identified as "Hispanic or Latino." The resulting difference of 2.2 percent, after subtracting from 102.2 percent, then corrects the overall percentage. The seemingly incorrect numbers are the result of overlapping identities.

[63] Watts, "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014."

[64] John Hudson, "U.S. Repeals Propaganda Ban, Spreads Government-Made News to Americans," *Foreign Policy*, July 13, 2013, available at <https://foreignpolicy.com/2013/07/14/u-s-repeals-propaganda-ban-spreads-government-made-news-to-americans/>.

[65] Michael Hastings, "Congressmen Seek to Lift Propaganda Ban," *Buzzfeed*, May 18, 2012, available at <www.buzzfeednews.com/article/mhastings/congressmen-seek-to-lift-propaganda-ban>.

[66] Harper Neidig, "Senators Introduce Bipartisan Privacy Bill," *The Hill*, April 24, 2018, available at <https://thehill.com/policy/technology/384550-senators-introduce-bipartisan-internet-privacy-bill>.

[67] "Social Media Privacy Protection and Consumer Rights Act of 2018," 115th Cong., S.2728, 2018, available at <www.congress.gov/bill/115th-congress/senate-bill/2728>.