Statement of

LAURA ROSENBERGER

Alliance for Securing Democracy, the German Marshall Fund of the United States

BEFORE THE UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE

Concerning

"Foreign Influence Operations and their use of Social Media Platforms"

August 1, 2018

Thank you Chairman Burr, Vice Chairman Warner, and Distinguished Members of the Committee for inviting me to address you today. Few issues are more important to the health and strength of our democracy than Americans' ability to engage freely in political speech, to hold vibrant debates free from manipulation, and to obtain reliable information about the issues of the day. And that's why America's adversaries are deliberately targeting those abilities.

I come at this issue as a national security professional who has watched social media and online platforms be weaponized to attack the foundations of our democracy. I watched from inside our National Security Council when Russia was test-driving many of these approaches in Ukraine as our government struggled to fully understand and respond to these tactics. And I watched from the campaign trail as our government was caught by surprise that these tools were being used against American democracy ahead of the 2016 presidential election.

Imagination Fails Again

Eighteen years ago, the 9/11 Commission report characterized the failures that led to that attack on our country as a "failure of imagination." I believe the failure to detect and disrupt the Russian government's weaponization of online platforms against the United States and our allies to be a similar failure to imagine – a failure not just by the government, but also by the very people who ought to understand these tools best: their creators.

Today, nearly two years after the alarm bells first began sounding about this activity, imagination is no longer required to understand this threat. Thanks in part to the bipartisan work of this Committee, we now know that social media and online information platforms have provided a powerful means for the Russian government to interfere in our democracy. But despite acknowledging and discussing this issue, meaningful efforts to close off these vulnerabilities by both government and the private sector remain woefully lacking. And I worry that even as we focus on the past, we are missing what still is happening at this very moment, and what will certainly happen again. What may have once been a failure to imagine is now a failure to act with the urgency and measures required to meet this threat to our democracy.

Virtual Tradecraft

Technology is not standing still, and authoritarian regimes – including not only the Russian government, but also others like the Chinese Communist Party, are learning lessons about how to use these tools most effectively.

Specific to Russia's efforts to target Americans, Russian government-linked actors have used a range of means to manipulate the information space: 1) using fake personas, websites, and automation to flood the information zone; 2) manipulating search results; 3) recruiting Americans to take action offline and using traditional media to spread manipulated content; 4) amplifying extreme content to increase polarization; 5) undermining faith in institutions, including the integrity of elections; 6) influencing public opinion directly, both in the U.S. and globally, in ways directly at odds with U.S. interests; and 7) spreading hacked and weaponized information.

While much focus appropriately has been on large social media platforms like Facebook and Twitter, they represent only a segment of the broader information ecosystem. The Russian government and its proxies have infiltrated and utilized nearly every social media and online information platform – including Instagram, Reddit, YouTube, Tumblr, 4chan, 9GAG, and Pinterest – flooding the information zone to target Americans. Some of these platforms have been used to target specific communities: Tumblr, for instance, was used to target African Americans. Paid advertising was combined with organic content to grow and build audiences, establish credibility, target content, and amplify certain messages. These accounts have also directed traffic to fringe websites created by foreign actors for the sole purpose of misleading Americans. For instance, the website "USAReally" was set up by an entity connected to the Russian Internet Research Agency (IRA) and claims to provide "objective and independent" news to Americans while focusing its content on divisive issues like guns, immigration, and LGBT rights.[1] While this site was amateurish and possibly meant to be discovered, numerous other fringe websites exist. Some of these sites and social media accounts have masqueraded as local news sites, attempting to establish themselves as credible community voices.[2]

Another way the Russian government distorts the information space is through manipulating search results. Just Google any geopolitical issue of significance to Moscow – MH-17, the White Helmets, the Novichok poisonings in the UK – and you will be served up a set of top results consisting of outlandish conspiracy theories emanating from Russia.[3] And on YouTube, while RT and Sputnik are labeled as "funded in whole or part by the Russian government," search results on similar geopolitical issues bring these channels to the top, and a

---

[1] Naira Davlashyan and Angela Charlton, "Russian Bots, Trolls Test Waters Ahead of US Midterms," *AP News*, July 15, 2018, https://www.apnews.com/9f85e68cd7764c9080e9edba089a5c16/Russian-bots,-trolls-test-waters-ahead-of-US-midterms.

[2] Tim Mak, "Russian Influence Campaign Sought To Exploit Americans' Trust In Local News," *NPR.Org*, July 12, 2018, https://www.npr.org/2018/07/12/628085238/russian-influence-campaign-sought-to-exploit-americans-trust-in-local-news.

[3] Bradley Hanlon, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," June 14, 2018, https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/.

millennial-focused RT spin-off, ICYMI, continues to operate without its Russian government affiliation labeled. Labeling some foreign government content but not all effectively lends more credibility to channels that remain unlabeled.

The Method to the Madness

What happens online doesn't necessarily stay online. We know that, using social media to masquerade as Americans, the IRA convinced Americans to set aside their daily activities and commitments to show up at protests.[4] Moreover, roughly nine out of ten of Americans currently get at least some of their news online,[5] and 67% get news from social media.[6] Social media also tends to drive what traditional media organizations cover, so manipulating the narrative online influences reporters' coverage offline. And disturbingly, according to one study, from 2015 to 2017, 32 major American media organizations – in a total of 116 articles – cited what we now know were fake IRA-created social media accounts masquerading as legitimate Americans.[7] This is not just a thing of the past – one IRA-created Twitter account, @wokeluisa, that was active through earlier this year appeared in more than two dozen news stories from outlets such as BBC, USA Today, Time, Wired, HuffPo, and BET.[8]

As you are aware, this manipulation has continued. Much of the activity today is aimed at amplifying discussion of contentious issues in order to further polarize American society. Fake accounts often jump on real debates happening in society to drive more attention to a particular issue, or to make certain extreme positions seem more prevalent than they actually are. Another goal of such activity is for these accounts and networks to insinuate themselves to a particular audience and gain followers by jumping on trending topics of discussion, for the purpose of later injecting views on other topics of particular interest to Russia. Non-political content has also been used for similar purposes. On Reddit, for example, a significant number of IRA-created accounts masquerading as Americans shared pornography and puppy photos,[9] and many also used handles from popular television shows, apparently to try to grow their audience.[10] This is a

---

[4] Tim Lister and Clare Sebastian, "Stoking Islamophobia and Secession in Texas -- from an Office in Russia," *CNN*, October 6, 2017, https://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html.

[5] "Digital News Fact Sheet," *Pew Research Center's Journalism Project*, June 6, 2018, http://www.journalism.org/fact-sheet/digital-news/.

[6] Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," *Pew Research Center's Journalism Project* (blog), September 7, 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

[7] Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets as Sources for Partisan Opinion: Study," Columbia Journalism Review, March 8, 2018, https://www.cjr.org/analysis/tweets-russia-news.php.

[8] Heather Gardner, "Twitter Does Not Respect Donald Trump Jr.'s Request for Privacy after Divorce Announcement," March 16, 2018, https://www.yahoo.com/entertainment/twitter-not-respect-donald-trump-jr-s-request-privacy-divorce-announcement-172804416.html.

[9] See, for example, https://www.reddit.com/user/emilyli and https://www.reddit.com/user/hank-schrade. Both accounts are among the 944 accounts Reddit suspended for association with the Internet Research Agency.

[10] Several handles used character names from the AMC television series "Breaking Bad," including saulgoodman1978, jessepinkman1984, salamanca_tuco, hank-schrade, fring-gus, and walterwhite1962.

sound strategy. After all, many of us forget why we followed someone on social media in the first place, but nonetheless continue to see their posts.

These operations often target both sides of a contentious issue – a pattern evidenced on Facebook,[11] Twitter,[12] and Reddit.[13] One IRA-created Twitter account that I mentioned earlier, @wokeluisa, was largely targeted at the left. In one viral tweet on the NFL Anthem protests that received 37,000 retweets, this IRA account tweeted on March 13, 2018 – just over fourth months ago: "Just a reminder: Colin Kaepernick still doesn't have a job, because in this country fighting for justice will make you unemployable." But at the same time, another IRA account, @BarbaraForTrump, was tweeting on the other side of this issue, consistently criticizing the Anthem protests.[14] An IRA-created Reddit account, mr_clampin posted similar remarks that President Obama was "telling us that we have no right to bear guns" in response to comments from Obama that Kaepernick was "exercising his constitutional right to make a statement."[15] In other words, the goal is not to influence the discussion in one particular direction, but rather to sow division and chaos across the political spectrum.

Another goal is to undermine faith in institutions. Russian active measures have sought to undermine public faith and confidence in the rule of law.[16] These attacks not only seek to weaken core pillars of democracy, but also to limit efforts to combat corruption and other pernicious activities that are endemic in autocratic societies.[17] IRA-created accounts have also played up concerns about potential vulnerabilities to U.S. election systems in order to undermine faith in elections.[18]

Russian-linked networks on social media also attempt covertly to influence public opinion and political sentiment in the United States and globally – on issues concerning both domestic and foreign policy. Sometimes, hot button or divisive issues serve as a platform to inject a geopolitical narrative. For example, a number of IRA-purchased ads on Facebook around the time of the Trump administration's May 2017 strikes on Syria following a chemical

---

[11] Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *The New York Times*, November 1, 2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

[12] Denise Clifton, "Russian Trolls Hyped Anger over Black Lives Matter More than was Previously Known," *Mother Jones*, January 30, 2018, https://www.motherjones.com/politics/2018/01/russian-trolls-hyped-anger-over-black-lives-matter-more-than-previously-known/.

[13] Caroline O., "Russian Propaganda On Reddit," Arc Digital, April 17, 2018, https://arcdigital.media/russian-propaganda-on-reddit-7945dc04eb7b.

[14] Donie O'Sullivan, "American Media Keeps falling for Russian Trolls," June 21, 2018, https://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

[15] Mr_Clampin, "Obama: Kaepernick 'exercising his constitutional right to make a statement,'" Reddit.com/r/politics,https://www.reddit.com/r/politics/comments/519c46/obama_kaepernick_exercising_his_constitutional/d7ah7ae/?context=3.

[16] Suzanne Spaulding, "Countering Adversary Threats to Democratic Institutions," Center for Strategic and International Studies, February 14, 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180214_Spaulding_CounteringAdversaryThreats_Web2.pdf?EzqGtMwOAjQIIH8eRNNoZ10T49OV63lh.

[17] Ibid.

[18] See e.g. an IRA-created Reddit account targeted at African-Americans: https://www.reddit.com/user/Abena_Tau

attack sought to influence public opinion against this military action.[19] One Facebook ad purchased by the fake IRA-created "Blacktivist" page and targeted at African Americans asked, "How would we feel if another country bombed us for the poisoned water in Flint and for police brutality?"[20] On Reddit, multiple IRA-generated memes posted to the r/funny sub-reddit were targeted at discouraging U.S. support for Montenegrin-accession to NATO, attempting to portray Montenegrins either as free riders or as protestors resisting this move.[21] These are just a few examples of the manner in which these information operations seek to use the community they have built around one set of issues to inject content that shapes American's foreign policy views. Another effort aims to shape Americans' views of Europe and Europeans' views of America more generally in a negative light – often using the debates around immigration as a means to do so. IRA-created accounts have promoted content from openly xenophobic sites, including an article that suggested that migrants from Muslim-majority countries were responsible for 84 percent of rapes in Sweden.[22]

This pattern is not unique to operations targeted at the United States. After the poisoning of former Russian spy Sergei Skripal and his daughter in the UK, Russian-language accounts on Twitter engaged in significant amplification of a poll which asked: "Are you satisfied that Theresa May has supplied enough evidence for us to be able to confidently point the finger of blame towards Russia?" UK officials believe that 2,800 Russian automated accounts were active on Twitter in Britain following the Skripal attack, reaching at least 7.5 million people.[23] A report released over the weekend by a UK Parliamentary Committee detailed Russia's use of social media for political interference in UK politics, including ahead of the Brexit referendum and the use of IRA-purchased political ads targeted at the UK.[24]

And while much attention has focused on the Internet Research Agency, we know that it was not the only Russian government-related actor using these tactics. In particular, from the Special Counsel's July 13 indictment of Russian GRU officers, we know that Russian military

---

[19] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed July 30, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm; U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 3023," Social Media Advertisements, accessed July 30, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[20] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 981," Social Media Advertisements, accessed July 26, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[21] IronhammerConjukelv, "Accession of Countries to NATO: expectations vs. reality," Reddit.com/r/funny/, https://www.reddit.com/r/funny/comments/3q5zpn/accession_of_countries_to_nato_expectations_vs/. and HityndiDutilar, "NATO? No action, talk only," Reddit.com/r/funny, https://www.reddit.com/r/funny/comments/3q5w97/nato_no_action_talk_only/.

[22] Shomyo, "Sweden: Migrants from Muslim-majority countries commit 84 per cent of very violent rapes," Reddit.com/r/uncen, https://www.reddit.com/r/uncen/comments/79ufdb/sweden_migrants_from_muslimmajority_countries/

[23] Deborah Haynes, "Skripal Attack: 2,800 Russian Bots 'Sowed Confusion after Poison Attacks,'" *The Times*, March 24, 2018, https://www.thetimes.co.uk/article/2-800-russian-bots-sowed-confusion-after-poison-attacks-zf6lvb3nc.

[24] United Kingdom House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report*, Fifth Report of Session 2017-19, July 29, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm.

intelligence officers also used fake social media personas and websites to spread weaponized information.[25] And the entities that have been uncovered and identified may be only the tip of the iceberg. At the same time, Moscow appears to be emboldened by its perceived success, and its activity is becoming more overt. After the Skripal attack, official Russian diplomatic Twitter accounts spread conspiracy theories, attacked critics, and mocked host-country government officials.

Manipulating Information as Authoritarian Tool

And it is not just Russia. The Chinese government has also begun to use social media to manipulate conversation and public opinion outside its borders, especially in its immediate region. The chat app LINE, popular in Taiwan, has been used to spread disinformation around politically sensitive issues; according to Taiwan national security officials, an increasing amount of this is from "content farms" located on the Chinese mainland.[26] In another instance, fake imagery of Chinese bombers flying near Taiwan's Jade Mountain circulated on the social media platform Sina Weibo in order to instill fear in the Taiwanese public – the image was shared widely before Taiwan's Defense Ministry denied the image.[27] China has also begun to censor content outside its borders, including via the popular Chinese chat app WeChat, as a means of shaping the information space.[28] China has pressured foreign tech companies to censor content on their platforms; in one case, Chinese authorities pressured Facebook to take down the account of a Chinese business tycoon living abroad because of content he posted critical of Beijing.[29]

As these examples show, while much of our discussion of social media manipulation in the United States has been in a political context, our authoritarian adversaries are using these tools because controlling the information space is a powerful means to advance their geopolitical goals. For them, this is a strategic domain, and social media and online information platforms are powerful weapons to be mastered and used to advance their interests and goals at the expense of democratic institutions and alliances. In the case of Putin's Russia, using information operations to weaken our democracy is a means for a declining Russia to gain relative power, and manipulating debate to promote a less-engaged America, a weaker NATO, and a weaker EU – all of which serve as counterweights to Moscow. In the case of Xi Jinping's China, denying the information space to its external critics and shaping discussion of institutions in a manner more favorable to Beijing will advance its goal of gaining a more dominant global position.

---

[25] Robert S. Mueller, III, United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, No. 1:18-cr-00215-ABJ (United States District Court for the District of Columbia July 13, 2018).

[26] Russell Hsiao, "CCP Propaganda against Taiwan Enters the Social Age," Jamestown China Brief 18, no. 7 (April 24, 2018), https://jamestown.org/program/ccp-propaganda-against-taiwan-enters-the-social-age/.

[27] Ibid.

[28] Lulu Yilun Chen, "WeChat Censoring Messages Even Outside China, Study Says," *Bloomberg*, November 30, 2016, https://www.bloomberg.com/news/articles/2016-12-01/wechat-censoring-user-messages-even-outside-china-study-says.

[29] Paul Mozer, "China Presses Its Internet Censorship Efforts Across the Globe," *The New York Times*, March 2, 2018, https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html.

Identifying Malicious Behavior Requires Information Sharing

That is why it is critical that we take meaningful steps – now – to address this problem and protect our country and our allies. We need to do so in a way that preserves our greatest strength – our free speech and privacy. Addressing this issue the right way will ultimately strengthen democracy. Moreover, this systemic problem requires action by the government, the private sector, and civil society.

The challenge of countering online information operations is usually discussed from one of two directions – either the content being promoted, or the actors' and their deceptive and manipulative intent and behavior. I believe that fundamentally, this is not a content problem. Looking at it this way misses large parts of activity in which malicious foreign actors are engaged, such as the use of fake personas and manipulation of search results; is a reactive approach by definition; and creates significant challenges with respect to free speech. Instead, I believe we must approach this issue as a deliberate manipulation of the information space by actors with malicious intent engaging in deceptive behavior. Focusing on the underlying behavior of the actors engaged in that activity helps identify patterns – making it easier to stop in the future.

There are several important steps that the government, tech companies, and civil society need to take to defend against and deter this behavior. These include: 1) information sharing between the public and private sector and among companies about malicious activity; 2) addressing identified vulnerabilities that have been exploited; 3) providing transparency about online activity, including disclosure of automated accounts and greater context for users about why they see certain content; 4) exposure of information operations; 5) collaboration with outside researchers; 6) adopting a proactive approach to identify new threats in technology before they are exploited; and 7) approaching this effort as part of a larger strategy to counter the full range of tactics authoritarian governments are using to undermine democracies.

Identifying malicious actors and their patterns of activity requires new mechanisms for data sharing, both between the public and private sectors and among technology companies. Government must play an important role in identifying the threat actors of concern. The intelligence community, in particular, has important capabilities that allow it to identify both the intentions and behaviors of threat actors. At the same time, social media companies have unique visibility in to activity on their platforms – and oftentimes government analysts cannot access that information. And given the manner in which these operations work across the information ecosystem, tech companies need to share threat indicators with one another.

The recently announced Department of Justice policy on foreign interference includes "Work[ing] with social media companies to illuminate and ultimately disrupt" foreign influence campaigns on their platforms," and a number of task forces have been set up across the government related to information sharing with social media.[30] These are welcome steps, which

[30] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download, 12.

need to be streamlined and institutionalized, and must include both vertical and horizontal information sharing that protects privacy and speech. There are models of such mechanisms from counter-terrorism, cybersecurity, and financial integrity efforts.[31]

One recent illustration of why this is so necessary is the case of a persona used by the GRU to masquerade as a left-leaning American journalist – Alice Donovan. According to the Special Counsel's June 13 indictment, the GRU used "a preexisting social media account under the name Alice Donovan" to create a Facebook page for DC Leaks, the site that was initially created and used to leak material hacked from the DNC.[32] According to press reports, the FBI began tracking "Alice Donovan" as a Russian government proxy/persona in the spring of 2016; reporters revealed that "she" may be a Russian troll in September 2017.[33] The Donovan persona's Facebook page remained live until the *New York Times* approached the company in September 2017.[34] The Twitter account was not suspended until *a few weeks ago* – after the Special Counsel's indictment, and months after Facebook's suspension and multiple press reports on the persona's suspected origin.[35] If these press reports are accurate, more robust information-sharing between the FBI and tech companies, and between Facebook and Twitter, could have resulted in earlier termination of this activity by Russian military intelligence.

Sunlight is the Best Firewall

Government and tech companies also need to close off vulnerabilities that have been and are being exploited. While organic content from foreign actors has had larger reach, the IRA exploited the lack of legal or regulatory requirements around political advertising online to purchase political ads, allowing them to target specific audiences with precision. While some companies have taken steps to implement their own transparency and disclosure requirements, others have not – and those that have acted have used different definitions for political

---

[31] One example is the Global Internet Forum to Counter Terrorism (GIFCT), whose goal is to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms by: employing and leveraging technology; sharing knowledge, information and best practices; and conducting and funding research. https://gifct.org/; The National Cyber Forensics and Training Alliance, is a nonprofit partnership between industry, government, and academia to provide a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime. http://www.ncfta.net/ ; Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) and the United States' FinCEN Exchange.

[32] Robert S. Mueller, III, United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, No. 1:18-cr-00215-ABJ (United States District Court for the District of Columbia July 13, 2018).

[33] Adam Entous, Ellen Nakashima, and Greg Jaffe, "Kremlin Trolls Burned across the Internet as Washington Debated Options," *The Washington Post*, December 25, 2017, https://www.washingtonpost.com/world/national-security/kremlin-trolls-burned-across-the-internet-as-washington-debated-options/2017/12/23/e7b9dc92-e403-11e7-ab50-621fe0588340_story.html?utm_term=.e1f173841821.

[34] Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times*, January 20, 2018, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

[35] Adam Entous, "The Rise and Fall of a Kremlin Troll," *The New Yorker*, July 19, 2018, https://www.newyorker.com/news/news-desk/the-rise-and-fall-of-a-kremlin-troll.

advertising and are implementing different restrictions on who can and cannot purchase them. Because disclosure and transparency provide consumers with important context to evaluate information, using different standards confuses consumers and could actually make the problem worse. Moreover, labeling publishers as political advertisers – as Facebook has – undermines users' faith in credible information. This is not an area for self-regulation – the need for a legal framework such as the Honest Ads Act that applies the same standards to political advertising online that apply on any other media could not be more clear.

Exposing information manipulation is critical to both reducing its effectiveness and deterring it. That is why transparency by the platforms about the actions they take is essential. To date, however, these companies have remained defensive about their approach to these issues, and much of what we know about the activity on them is only due to the pressure from this Committee and others in Congress. The focus cannot be on public relations campaigns about tech companies' commitment to addressing the problem – it needs to be on detailing the nefarious activity these companies are seeing and curtailing.[36]

Government must play a similar role in publicly exposing foreign interference activity on social media. The recently announced Department of Justice policy to alert key individuals, including victims, tech companies, Congress, and the public about foreign influence activities is a welcome development.[37] As much as possible, information should be provided in an unclassified format to enable non-government actors to more readily act on it. But as we saw in 2016, too often this issue becomes ensnared in politics – which will limit an effective response. Legislating mandatory reporting requirements for DNI and DHS would be a critical step to ensure that approach going forward. I appreciate the consideration of such measures in the Intelligence Authorization Act, and hope they will be enacted and include the full scope of foreign interference activity that we are discussing today.

Transparency by tech companies on the actions they are taking is also critical for accountability. It is essential that outside researchers be given greater access to data – in a manner that protects users' privacy – in order to have greater visibility into the activity on these platforms and inform development of strategies to address malign activity. While some companies have taken steps along these lines, they remain too limited and narrow to have a real impact. Civil society should be seen as an ally – not an adversary – in countering foreign actors' manipulation of social media.

Transparency also means providing users with more information about the origin of information and why they see it, as context is critical to evaluating information. Senators Warner and Rubio wrote recently that "there is really no better defense against Russian

---

[36] Paul M. Barrett, Tara Wadhwa, and Dorothée Baumann-Pauly, *Combating Russian Disinformation: The Case for Stepping Up the Fight Online* (New York, NY: NYU Stern Cetner for Business and Human Rights, July 2018).
[37] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download.

aggression on social media than an informed citizenry."[38] Transparency around and disclosure of automated accounts is another means to ensure consumers have information about the online information space. Any such disclosure requirements should ensure that anonymity online – which remains an important and empowering force for activists in authoritarian countries – remains protected even while disclosing those accounts that are automated.[39] Longer-term, media literacy and critical thinking skills are essential to promoting resilience, but these efforts do not address how the information space itself is manipulated to make certain content seem more prevalent than it is. Any media literacy efforts need to include online literacy, so people can be more critical in assessing not just the information they are seeing but *why* they are seeing it. Education outreach must also extend beyond classrooms, as research suggests that older generations may be more vulnerable to digital disinformation.[40]

Getting Ahead of the Curve

To ensure that imagination does not fail us again, we need to develop better mechanisms to identify threats in new technology before they are exploited, including through greater connectivity between the national security and tech communities. For too long, "move fast and break things" has been tech's modus operandi, with any downsides of technological creation to be addressed once a product released into the wild.

That approach needs to change. As Alex Stamos, the departing CSO at Facebook, told his colleagues: "we need to think adversarially in every process, product and engineering decision we make."[41] We know that AI will present both new tools to combat the problem of information manipulation as well as new ways to make it much worse – such as "Deep Fakes," which use AI to manipulate video and audio content so that it is indistinguishable to the human eye or ear. Moreover, the growth of the Internet of Things will increase the surface area for cyberattacks, due to the increased number of exploitable Internet-connected devices Americans are placing in their homes, offices, and on their roads. It is critical that we get ahead of these threats – and others we have likely not yet identified, before they are weaponized against us.

Seeing the Whole Field

Finally, foreign actors' manipulation of social media is part of a larger strategy to undermine our democratic institutions. The bipartisan organization I co-direct recently released a "Policy Blueprint for Countering Authoritarian Interference in Democracies," which outlines a

---

[38] Mark Warner and Marco Rubio, "As Trump Meets Putin, We'll Spotlight and Resist Russian Aggression: Warner & Rubio," *USA TODAY*, July 12, 2018, https://www.usatoday.com/story/opinion/2018/07/12/trump-putin-helsinki-summit-resist-russian-aggression-column/776617002/.

[39] One option for requiring such disclosure is S.3127 - Bot Disclosure and Accountability Act of 2018," *Congress.gov, www.congress.gov/bill/115th-congress/senate-bill/3127*.

[40] David Z. Hambrick and Madeline Marquardt, "Cognitive Ability and Vulnerability to Fake News," *Scientific American*, February 6, 2018, https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/.

[41] Ryan Mac and Charlie Warzel, "Departing Facebook security officer's memo: 'We need to be willing to pick sides,'" *Buzzfeed*, July 24, 2018, www.buzzfeednews.com/article/ryanmac/facebook-alex-stamos-memo-cambridge-analytica-pick-sides.

comprehensive strategy that was endorsed by a bipartisan and transatlantic group of former senior national security officials (See Appendix A).[42] Among those recommendations, our government needs to send clear deterrent warnings to foreign actors about the costs that will be imposed for engaging in such activity – including through additional sanctions like those proposed in the DETER Act and the legislation being developed by Senators Graham and Menendez[43] – and identify our own asymmetric advantages.

As we were again reminded by recent reports about alleged cyberattacks on several Congressional candidates, including reportedly Senator McCaskill, cyberattacks remain a core part of the Russian government's arsenal. That is why we need to harden our election systems against cyber threats through measures like the SECURE Elections Act. Such steps are also critical to ensuring that Americans have confidence in our election systems, as information operations casting doubt on the credibility of an election could undermine faith in the outcome even if those systems themselves are not compromised. And more broadly, the government needs to develop a unified and integrated approach to this issue in order to see and respond to the full threat picture – this should include a creating a counter-foreign interference coordinator at the National Security Council and a National Hybrid Threat Center.

At its core, this is a transnational challenge. Our European partners and allies have experiences from which we can learn, and it is essential that we work more closely together through mechanisms like that established at the recent G7 meeting[44] to share information about threats and collaborate on responses to this shared challenge to our democracies. The UK report released earlier this week outlines the hurdles it has faced in getting transparency and action from tech companies, as well as the kinds of measures it is considering.[45] We will be more powerful in tackling these shared challenges if we do so together.

Distinguished Members, robust action from tech companies, Congress, the Executive Branch, and civil society are all required to meet these threats to our democracy. While this is not an easy issue, there are clear steps that we CAN take – today – to make our democracy more secure. We need to come together as Americans – across party lines and between the public and private sector – to address this challenge. Putin's strategy is to divide Americans from one another in order to weaken us as a country. A partisan response to this issue only help Putin succeed. It is imperative that we stand as a united front against these threats to our country, and

---

[42] Jamie Fly, Laura Rosenberger, and David Salvo. *Policy Blueprint for Countering Authoritarian Interference in Democracies.* June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

[43] See United States Congress, Senate, *Defending Elections from Threats by Establishing Redlines Act of 2018*, S 2313, 115th Cong., 1st. sess., introduced in Senate January 16, 2018, www.congress.gov/bill/115th-congress/senate-bill/2313; see also Jordain Carney, "Graham, Menendez Crafting Bill to Crack down on Russia," *The Hill*, July 24, 2018, http://thehill.com/homenews/senate/398583-graham-menendez-crafting-bill-to-crack-down-on-russia.

[44] Leaders of the Group of Seven, "Charlevoix Commitment on Defending Democracy from Foreign Threats," June 9, 2018, https://g7.gc.ca/wp-content/uploads/2018/06/DefendingDemocracyFromForeignThreats.pdf.

[45] United Kingdom House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report*, Fifth Report of Session 2017-19, July 29, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm.

that we reduce the polarization and real issues at home that Putin is exploiting. In the face of this threat, standing together as Americans has never been more important.

Appendix A

Jamie Fly, Laura Rosenberger, and David Salvo. *Policy Blueprint for Countering Authoritarian Interference in Democracies.* June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf