S. HRG. 115–397

OPEN HEARING ON FOREIGN INFLUENCE OPERATIONS' USE OF SOCIAL MEDIA PLATFORMS (THIRD PARTY EXPERT WITNESSES)

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

WEDNESDAY, AUGUST 1, 2018

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–959 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN III, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

AUGUST 1, 2018

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

OPEN HEARING ON FOREIGN INFLUENCE OPERATIONS' USE OF SOCIAL MEDIA PLATFORMS (THIRD PARTY EXPERT WITNESSES)

WEDNESDAY, AUGUST 1, 2018

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Warner, Risch, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, and Harris.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call the hearing to order.

I'd like to welcome our witnesses today: Dr. Todd Helmus, Senior Behavioral Scientist at the RAND Corporation; Renee DiResta, Director of Research at New Knowledge; John Kelly, CEO and founder of Graphika; Laura Rosenberger, Director of the Alliance for Securing Democracy at the German Marshall Fund; and Dr. Phil Howard, Director of the Oxford Internet Institute.

Welcome to all of you. I thank you for being here today and for your willingness to share your expertise and insights with this Committee and, more importantly, with the American people.

We're here to discuss a threat to the Nation that this Committee takes every bit as seriously as terrorism, weapons of mass destruction, espionage and regional instability. Today we're talking about how social media platforms have enabled foreign influence operations against the United States.

Every member of this Committee and the American people understand what an attack on the integrity of our electoral process means. Election interference from abroad represents an intolerable assault on the democratic foundation this republic was built on.

The Committee, in a bipartisan fashion, has addressed this issue head on. In May, we released the initial findings of our investigation into Russia's targeting of election infrastructure during the 2016 election.

Today's hearing is an extension of that effort. But in some ways it highlights something far more sinister, the use of our own rights and freedoms to weaken our country from within. It's also impor-

tant that the American people know that these activities neither began nor ended with the 2016 election. As you can see on the one graph on display to my left, your right, the Kremlin began testing this capability on their domestic population several years ago, before using it against their foes in the Near Abroad and on the United States and Western democracies.

Even today, almost two years after the 2016 election, foreign actors continue an aggressive and pervasive influence campaign against the United States of America. Nothing underscores that fact more than yesterday's announcement by Facebook that they've identified over 30 new accounts that are not only causing chaos in the virtual domain, but also creating events on our streets with real Americans unknowingly participating.

These cyber actors are using social media platforms to spread disinformation, provoke societal conflict and undermine public faith in democratic institutions. There does not seem to be much debate about that.

I think it's also the case that social media isn't going anywhere anytime soon. It's part of how we exchange ideas, we stay connected, it binds us as a community, it gives voice to those that are voiceless. Social media is the modern public forum, and it's being used to divide us.

This was never about elections. It is about the integrity of our society.

So how do you keep the good while getting rid of the bad? That's the fundamental question in front of this Committee and in front of the American people. And it's a complex problem that intertwines First Amendment freedoms with corporate responsibility, government regulation and the right of innovators to prosper from their own work.

Sixty percent of the U.S. population uses Facebook. A foreign power using the platform to influence how Americans see/think about one another is as much a public policy issue as it is a national security concern.

Crafting an elegant policy solution that's effective but not overly burdensome demands good faith and partnership between social media companies and this Committee. We hope to hear from those innovators in September, because you can't solve a problem like this by imposing a solution from 3,000 miles away. This requires a thoughtful and informed public policy debate and this Committee is uniquely positioned to foster that debate.

Last November, when we first welcomed the social media companies in an open hearing, I stressed then what this debate is and is not about. This isn't about relitigating the 2016 U.S. presidential elections. This isn't about who won or who lost. This is about national security. This is about corporate responsibility. And this is about the deliberate and multifaceted manipulation of the American people by agents of a foreign hostile government.

I thank you again for being here, for the work that you've done. Your analytic and technical expertise is indispensable to us getting this right. We cannot possibly formulate the right solution without first knowing the extent of the problem.

I'm hopeful this morning that as you offer your insights and your findings, that you'll also share your recommendations. We can't afford ineffective half-measures, let alone nothing at all.

While it's shocking to think that foreign actors used social networking and communication mediums that are so central to our lives in an effort to interfere with the core of our democracy, what is even more troubling is that it's still happening today. Nothing less than the integrity of our democratic institutions, processes and ideals is at stake.

With that, I turn to the Vice Chairman.

OPENING STATEMENT OF HON. MARK R. WARNER, VICE CHAIRMAN, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman, and I also want to welcome our witnesses today.

This Committee has invested a significant amount of time, focus, and energy, both in public and behind closed doors, in uncovering and exposing Russian information warfare in our own backyard.

It is clear that our efforts have increased Americans' understanding of what the Russians did in 2016 and how they sought to attack us through the use of social media. It was pressure brought by this Committee that led Facebook, Twitter and YouTube to uncover malicious activity by the Russian-backed Internet Research Agency. These revelations eventually resulted in the indictments of 13 Russian individuals and three Russian companies by the Special Counsel's Office in February of this year.

Social media oversight has not typically been a function of our Committee and, for that matter, any Committee. I have no problem acknowledging that the terminology of this world—bots, spam, click bait, API, trolls—does not always come naturally to all of us. But thanks to bipartisan determination to understand what happened in 2016 and a commitment to stopping it from happening again, we have been able to accomplish a lot. We have helped reveal the Russian playbook, we have raised public awareness regarding the threat, and we have succeeded, however incremental, in pressuring each of these companies to take steps to address the problems on their platforms.

That's the good news. The bad news is that we've got a lot more work to do. Twenty-one months after the 2016 election and only 3 months before the 2018 elections, Russian-backed operatives continue to infiltrate and manipulate social media to hijack the national conversation and set Americans against each other. They were doing it in 2016; they are still doing it today.

That was made just evident yesterday, as the Chairman noted, when Facebook announced the takedown of 32 new pages and accounts that had connections to Russian-backed operations, and those accounts had hundreds of thousands of followers.

In our previous hearings on Russian disinformation, we outlined the Russian playbook in the 2016 elections. We discussed how Russian operatives set up thousands of fake and automated accounts on Facebook, Instagram, Twitter, YouTube and others, in order to build networks of hundreds of thousands of real Americans. These networks pushed an array of misinformation, including stolen e-mails, state-led propaganda, fake news and divisive content, onto

the newsfeeds of as many potentially receptive Americans as they could. And you will note out here today from our experts that they were extremely successful in that effort.

These active measures have two things in common: first, they're effective; and second, they're cheap. For just pennies on the dollar, they can wreak havoc in our society and in our elections.

And I'm concerned that, even after 18 months of study, we are still only scratching the surface when it comes to Russia's information warfare. Much of the initial focus was on paid advertisements, but it quickly became clear that these ads represented a tiny percentage of the IRA's activity compared to the hundreds of thousands of free Facebook and Instagram posts, pages and groups, and millions of tweets from IRA-backed accounts.

Today, it is becoming clearer that IRA activity represents just a small fraction of the total Russian effort on social media. In reality, the IRA operatives were just the incompetent ones who made it easy to get caught. Who else is still out there actively attacking us? Are there other troll farms? What about the actual Russian intelligence services? I hope we'll hear from the experts today how much further out they think this Russian disinformation effort goes.

I'm also concerned that the United States government is not well-positioned to detect, track or counter these types of influence operations on social media. These types of asymmetric attacks—which include foreign operatives appearing to be Americans, engaging in online public discourse—almost by design slipped between the seams of our free speech guarantees and our legal authorities and responsibilities.

Again, I hope our witnesses will recommend ideas for better tackling this problem while also protecting our constitutional rights as Americans.

All the evidence this Committee has seen to date suggests that the platform companies, namely, Facebook, Instagram, Twitter, Google and YouTube, still have a lot of work to do. Now, before I went into politics I spent more than 20 years in the tech business and I have tremendous respect for these companies and what they represent. And when they are at their best, they are a symbol of what this country does best: innovation, job creation, changing the world.

I've been hard on them, though, that's true. But it's because I know they can do better to protect our democracy. They have the creativity, expertise, resources, and technological capability to get ahead of these malicious actors.

That's why, as the Chairman mentioned, we'll be hosting senior executives from Facebook, Twitter, and, yes, Google, for a hearing on September 5th to hear the plans they have in place, to press them to do more, and to work together to address this challenge.

That's because it's only going to get harder. As digital targeting continues to improve, and as new advances in technology and artificial intelligence—one that I'm particularly concerned on, like deep fakes—continue to spread, the magnitude of the challenge will only grow.

I know today we'll focus on what happened in 2016 and what is happening now, but Russian active measures have revealed a dark

underbelly of the social media ecosystem. These same tools that spread misinformation can negatively affect other aspects of our lives.

I think we need to start pushing ourselves beyond just recognizing the problems and start to press actual policy ideas forward. I'm interested in hearing some of those policy options that might help us address broader challenges posed by the growth and dominance of a few social media companies.

For example, does a user have the right to know if they are interacting with a person or a bot online? Do companies have a responsibility to ensure more transparency of how they collect, use, and secure user data? Do users have enough control over their own personal data?

I hope, as a panel of experts here, you can help this Committee to lead and to begin to shape a bipartisan responsibility to this ongoing, as the Chairman has indicated, national security threat.

Thank you, Mr. Chairman.

Chairman BURR. I thank the Vice Chairman.

Before I move to the testimony from our witnesses, some Committee housekeeping. After testimony, members will be recognized for five minutes by seniority, and I will hold that to five minutes today.

We have five votes that are scheduled for 11 a.m. I'll make sure that all members today are able to ask these witnesses their questions. I would ask members that, when you need to leave to vote, would you be expeditious in coming back if you're in the queue to ask questions, and the Chair will work with each one of you to let you know where we think you'll be in the sequence.

The Chair will announce he's going to miss the first two votes to stay here and keep the continuity of the hearing going so that we can get through as many members as we possibly can.

With that, Dr. Helmus, I'll recognize you and we'll go from your right to left from there on. Dr. Helmus, the floor is yours.

STATEMENT OF TODD HELMUS, Ph.D., SENIOR BEHAVIORAL SCIENTIST, RAND CORPORATION

Dr. HELMUS. Thank you, Chairman.

Good morning, Chairman Burr, Vice Chairman Warner and distinguished members of the Committee. Thank you for the invitation to testify at this important hearing.

Russia is engaged in a worldwide propaganda campaign. One particular focus for this campaign is in Russia's own backyard, in the former Soviet states of Eastern Europe. In addition to a military and propaganda war in Ukraine, Russia is disseminating propaganda to Russian speakers in the Baltics and other nearby states.

Their goal principally is to drive a wedge between these Russian speakers and their host nations, the North Atlantic Treaty Organization, and the European Union. To do this, Russia uses—Russia, of course, uses bot and troll social media accounts. They also synchronize such tools with their state-funded television network, their online news portals, and an army of regional proxies that some call "useful idiots."

The RAND study I will talk to you about today sought to better understand the nature and effectiveness of Russian—of pro-Russia outreach on social media. By focusing on the region that includes Estonia, Lithuania, Latvia, Ukraine, Moldova, Belarus, our research team sought to help advance NATO's defense of the Baltic states and shed light on how to combat this issue around the globe. My written testimony highlights the analytic methods and key findings from this—from our report, but for today's testimony, I'll focus on our five key recommendations.

First, there's a need to further develop analytic methods to track and target Russian propaganda efforts. To take any action against Russian social media operations, it is critical to identify Russian bot and troll accounts and track their activity in real time. This will require continued analytic advancements so that computers can distinguish between authentic social media chatter and the adversarial information campaigns that are to come.

Second, it is important to highlight and tag Russian propaganda. The approach by international organizations involves frequently websites or e-mail alerts which reach only fellow activists or members of the policy community. Instead, the research team argues that it is important to highlight Russian propaganda in ways that are much faster and target at-risk audiences.

One example is Google ads could potentially help improve the speed and targeting of counter-messaging. The approach uses videos and other content embedded in Google search results to educate people who search for Russian-born fake news on Google.

Third, expand and improve access to local and original content. One challenge, particularly in the Baltics, is that Moscow-controlled media, especially TV, is a dominant source of information for many Russian speakers in the region. Policies should not so much counter the Russian narrative as to displace it with more entertaining and accurate content. The team argues for training Russian language journalists, increasing access to Russian language television programming such as Current Time, and highlighting the authentic voice of local influencers.

Fourth, the U.S., NATO and the EU must do a better job of telling their story. They should, for example, offer a compelling argument for Russian-speaking populations to align with the West or individual nation-states to which they belong. NATO should also more effectively communicate the purpose and intent of its infantry battalions now stationed in the Baltics.

Finally, there is a need to build resilience in target populations. This will include long-term effort to implement media literacy training and integrate such training into classrooms. A public information campaign that can immediately convey the concepts of media literacy and the risk of Russian propaganda may also be necessary.

Thank you once again for inviting me, and I look forward to taking your questions.

[The prepared statement of Dr. Helmus follows:]

Russian Social Media Influence

Understanding Russian Propaganda in Eastern Europe

Todd C. Helmus

CT-496
Testimony presented before the Senate Select Committee on Intelligence on August 1, 2018.

For more information on this publication, visit www.rand.org/pubs/testimonies/CT496.html

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe

Testimony of Todd Helmus[1]
The RAND Corporation[2]

Before the Select Committee on Intelligence
United States Senate

August 1, 2018

Good morning, Chairman Burr, Vice Chairman Warner, and distinguished members of the committee. Thank you for the invitation to testify at this important hearing.

Russia is engaged in an active, worldwide propaganda campaign. Information operations are a major part of Russia's foreign policy and social media are one important element of Russia's state-led activities. The RAND Corporation has been studying these activities; today, I will share some lessons learned from one particular study—*Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*—that examined Russia's social media influence in Eastern Europe.[3] Understanding activities in this region, which Russia considers its "near abroad," will help advance the North Atlantic Treaty Organization (NATO) defense of the Baltics and also shed light on how to combat this issue around the globe. I will provide an overview of Russian propaganda activities, review our efforts to identify Russian propaganda on Twitter, and examine challenges confronting U.S. and European policymakers in the region. I will conclude with recommendations for countering the Russian propaganda threat.

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

[3] Todd C. Helmus, Elizabeth Bodine Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018.

Overview of Russian Propaganda Activities

The Kremlin has made significant investments to influence the social media debate, developing an army of trolls, or fake social media accounts managed by Russian agents, as well as social media bots, or automated social media accounts.[4] These capabilities, initially designed to influence the Russian domestic audience, have likely been adapted and expanded to be used abroad.

This social media does not work in isolation but is part of a larger propaganda infrastructure. A state-funded Russian television network, *Russia Today* (*RT*), broadcasts abroad in English, Arabic, and Spanish. State-controlled news websites, such as *Sputnik*, disseminate news in about 30 languages. Russia also relies on civil society organizations, political parties, think tanks, and private citizens to echo and reinforce the Kremlin message.[5] Some of these elements may be directly supported by the Russian state; others disseminate pro-Russia content on their own free will and dime. Russia's social media campaigns are often synchronized tightly with these outlets.

The objectives for social media campaigns vary. In the former Soviet states, including the Baltic states and Ukraine, the Kremlin often aims to leverage shared elements of the post-Soviet experience to drive wedges between ethnic Russian and Russian-speaking populations and their host governments, NATO, and the West. Further abroad, the Kremlin often attempts to achieve policy paralysis by sowing confusion, stoking fears, and eroding trust in Western and democratic institutions. To achieve these and other objectives, Russian social media operations work on many fronts, including influencing conversation and debate on news comment sections; organizing protests against adversary governments, such as Ukraine; increasing web traffic for state-sponsored news stories; harassing individuals who criticize the Russian state; and disseminating fake news and other propaganda content.[6]

Although Russia seems to have a near-worldwide scope to its propaganda campaign, it is particularly interested in the lands on its western border—part of what Russia calls its "near abroad." This region stretches from the Baltic states to Ukraine and encompasses Estonia, Latvia, Lithuania, Belarus, and Moldova. This is an area of intense Russian focus, as evidenced by Russia's annexation of Crimea; the ongoing hybrid warfare in eastern Ukraine; and a campaign

---

[4] Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," Chatham House, Russia and Eurasia Programme, March 21, 2016.

5 See John Lough, Orysia Lutsevych, Peter Pomerantsev, Stanislav Secrieru, and Anton Shekhovtsov, "Russian Influence Abroad: Non-State Actors and Propaganda," Chatham House, Russia and Eurasia Programme Meeting Summary, October 24, 2014; Daunis Auers, *Comparative Politics and Government of the Baltic States: Estonia, Latvia and Lithuania in the 21st Century*, New York: Palgrave Macmillan, 2015; and Andrew Wilson, "Four Types of Russian Propaganda," *Aspen Review*, Issue 4, 2015.

6 A number of examples support these points. In January 2016, automated complaints posted by bots on social media caused Twitter to block pro-Ukraine user accounts. Russia also used themed groups on such social media platforms as the Russian-language VKontakte (similar to Facebook) to mobilize antigovernment protests against the Ukrainian government. It also used social media to spread fake rumors to undermine the morale of Ukrainian troops and discredit Ukrainian leadership and sent harassing SMS messages to Ukrainian soldiers on Ukraine's eastern front. Russia also used trolls and bots to artificially inflate web traffic and statistics for pro-Russia content. See Giles, 2016; Digital Forensic Research Lab, Atlantic Council, "Electronic Warfare by Drone and SMS: How Russia-Backed Separatists Use 'Pinpoint Propaganda' in the Donbas," *Medium.com*, May 18, 2017; and Landana Samokhvalova, "The Russian Organizers of a 'Third Maidan' in Ukraine," *Euromaidan Press*, February 14, 2016.

of fake news, hostile Twitter bots, and encouraging protests. Neighboring countries look at these actions and wonder where Russia will turn next.[7]

The Office of the Secretary of Defense's Rapid Reaction Technology Office asked the RAND Corporation to help it better understand the nature and effectiveness of pro-Russia outreach on social media and identify countermessaging opportunities in the areas surrounding Russia. The goals of our study of Russian social media influence were to (1) identify pro-Russia propagandists and anti-Russia activists on Twitter; (2) assess the degree to which Russian-speaking populations in a selection of former Soviet states have adopted pro-Russia propaganda themes in their Twitter language, and (3) consider challenges confronting U.S. and European policymakers in the region.

Identify Pro-Russia Propagandists and Anti-Russia Activists on Twitter

By analyzing Russian-language Twitter data emanating from the former Soviet states of Estonia, Latvia, Lithuania, and Ukraine, as well as from Moldova and Belarus, we were able to uncover two communities of interest—a population of pro-Russia activists and a community of Ukrainian activists.[9] These communities were not only large, with approximately 40,000 members each, but also highly influential. They produced a lot of content and were mentioned by a large number of accounts. When we examined this content, we discovered that these communities form two sides of a war of ideas.

The Russian activist community consisted of consumers and disseminators of pro-Russia propaganda. They disseminated content that was virulently anti-Ukraine and the West, and they supported breakaway Ukrainian confederations aligned with Russia. The Ukrainian activist group appeared to oppose Russian interference and exposed Russian propaganda. They supported Ukrainian independence and opposed corruption.

We also analyzed the key influencers of each community. For the pro-Russia community, the most influential users were ardently pro-Russia and anti-Ukraine and the West. Several disseminated what are described as "hate posts" about Ukraine and the United States, and one pontificated on Russian history. Several influencers appeared to operate from Russia or pro-Russia locations, and one was a journalist based out of the United Kingdom. Pro-Ukraine

---

7 Russia has several reasons for training its propaganda machine on the former Communist countries. First, effectively influencing the political outcomes of these countries helps establish a cushion against what it considers malign Western influence. Second, some of these countries, including the Baltic states and Ukraine, have minority populations of Russian-speaking former Soviet citizens and their descendants. It is an established Russian policy—specifically, "the compatriot policy"—to protect the interests of this population and, more importantly, influence this population to support pro-Russia causes and effectively influence the politics of its neighbors. See Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses*, Santa Monica, Calif.: RAND Corporation, RR-1577-AF, 2017.

9 Using a method called Community Lexical Analysis, or CLA, we conducted social network analysis of our Twitter data set to distill 22,825,114 Russian-language tweets from 512,413 unique user accounts into ten of the most central or influential communities. We then used a analytics software called RAND Lex, which identifies statistically overpresent and underpresent words in comparison to a baseline text. For this study, our baseline text included all Russian-language tweets in our collected dataset. For more on RAND Lex, see Elizabeth Bodine-Baron, Todd Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016.

influencers were, of course, anti-Russia and pro-Ukraine. Several used humor and sarcasm to convey their message, and others sought to expose Russian propagandists and fake news content. One was even supported by Radio Free Europe, in a type of capacity-building venture that is proposed in the recommendations of our recent research. Our study argues that analyses such as these can play a key role in campaigns designed to empower anti-Russia influencers.[10]

Are the accounts in the pro-Russia activist community working at the behest of the Russian state? We ran a randomly selected 2,000 accounts from each community to determine whether they were computer automated.[11] Accounts are more likely to exhibit bot-like behavior in the pro-Russia than in the pro-Ukraine activist community at a statistically significant rate, although the total numbers remain under 10 percent for both groups. Either the Russian activist community has fewer Russian bots than anticipated, or the Russians have improved their ability to surreptitiously field social media bots.[13] Alternatively, the accounts could be managed by Russian troll accounts, but such accounts can be difficult to distinguish from Russia's zealous, but otherwise authentic, base. Being able to differentiate Russian state-sponsored propaganda campaigns from genuine Twitter content is a key and challenging question for technologists.

The Degree to Which Regional Twitter Users Have Adopted the Language of Pro-Russia Propagandists

We tested whether we could discern the influence of the pro-Russia activist community over time and in different regions in eastern Europe. To do this, we developed a fingerprint of the word patterns from the content from the pro-Russia activist community. We then compared that word pattern fingerprint with that of eight longitudinal panels of Twitter users who were geo-inferenced to the region.[14]

The team found that an extremely high 15 to 20 percent of users in Crimea and Donetsk shared the same linguistic pattern as the rabid pro-Russia activist Twitter community. This rate drops the farther one goes away from the zone of Russian influence.[3] Only approximately 5

---

[10] Identifying these influencers—as well as the number of followers and what each is focusing on—is useful for targeting and countermessaging. For example, if the U.S. government were to work with pro-Ukraine influencers and help improve their skills, it could more effectively counter the Russian propaganda machine. It goes without saying that the pro-Ukraine influencers have far more credibility than any U.S. government agency.

11 Such features include unusual frequency of tweets, profile characteristics, and retweet behavior; Botometer, home page, undated.

13 The field of computer bots is engaged in an arms race with bot developers increasingly trying to create bots that mimic complex human behavior on social media and can avoid detection by automated bot detector programs. See Jinque Zhang, Rui Zhang, Yanchao Zhang, and Guanhau Yan, "The Rise of Social Botnets: Attacks and Counter Measures," *IEEE Transactions on Dependable and Secure Computing*, March 8, 2016.

14 The data for the panels consisted of all tweets that met all of the following conditions: (1) They were written between August 2015 and May 2016, (2) they contained primarily Russian language (according to Gnip's language classification algorithm), (3) they belonged to one of the 2,200- to 2,600-person user samples in six specific areas in Ukraine (Crimea, Donetsk, Dnipro, Kharkov, Kiev, and Odessa) and two other areas in the region (Minsk and Riga). These samples yielded between 500,000 and 900,000 tweets each.

percent of users reporting from Kiev, Minsk, and Riga, show similarities to the Russian activist community.

We validated the ability of our method to accurately detect the pro-Russia activist accounts and argue that this method could be used to track the spread of Russian propaganda over time in various regions. This could be a critical component to an effort to detect malign Russian information-shaping campaigns in real time.

Challenges Confronting U.S. and European Policymakers in the Region

To understand threats and identify policy recommendations, we interviewed more than 40 U.S. and regional experts for our study, visited U.S. European Command in Stuttgart, and met with security and civil society experts in Estonia and Latvia.

We learned several lessons from these engagements. First, given the breadth of Russia's propaganda campaign, it should not be surprising that it is not solely a social media problem. Particularly for the Baltic states of Estonia, Latvia, and Lithuania, the biggest propaganda threat comes from television. Moscow-controlled media, especially television, is the dominant source of information for many Russian speakers in the countries of the former Soviet Union.[15] Any effort to address Russian propaganda in the region must account for this monopoly that Russia holds over the Russian-language media market.

Second, the intensity of Russia's information campaign on social media appears higher in Ukraine than in the Baltic states. Some Baltic government security experts suggest that they are worried about an intensified Russian social media propaganda as a prelude to a kinetic campaign.

Third, there is a relatively high presence of Russian-speaking populations in the region. They are or descend from Soviet-era migrants, and their host countries have refused them citizenship—giving Russia a unique opportunity to communicate with a sympathetic audience. Further, some government policies prioritize national languages and limit government outreach in the Russian language, complicating state outreach to Russian speakers.

Finally, as discussed above, numerous social media activists, websites, news sources, and other content producers appear to actively disseminate their own pro-Russia propaganda without any obvious direct support from the Russian state. This makes identification of state-sponsored Russian-language bots, trolls, and other nonattributed content difficult.

Recommendations

Drawing on the above, our study made five recommendations that seek to limit Russian influence in the region.

Expand and Improve Access to Local and Original Content

To effectively compete with Russia propaganda, it is critical that Russian speakers in the region have alternatives to Russian-language television, Internet, and social media entertainment.

---

15 Ukraine is the exception: It has censored Russian government broadcasting and VKontakte.

The key is not to so much counter the Russian narrative as to displace it with more entertaining and accurate content. There are several options for achieving this objective.

One approach is to empower influencers on social media. There are many social media activists in the region who speak Russian, hold pan-European outlooks, and have a large following on social media. The goal is to identify such actors and provide funding for content creation; offer training in monetization; and, overall, help them produce better content. Some efforts are ongoing in this respect, and additional efforts are needed.

Alternatively, some people we spoke with in the region suggested formal training efforts for Russian-speaking journalists in the region. Others suggest increasing access to Russian-language television programming. The Estonians, for example, have begun a publicly funded television station to help communicate to the 300,000 Russian-speaking residents of Estonia. The United States has created *Current Time*, a Russian-language television broadcast that seeks to give the U.S. perspective on news and current events. *Current Time* may also wisely increase their portfolio of entertainment programming.

Better Tell the U.S., NATO, and European Union Story

NATO, European Union, and host nations should offer a compelling argument for Russian-speaking populations to align with the West or with individual nation-states; populations, especially those sitting on the fence, should be easily able to grasp the goals and motivations of the West. Our study concludes that such a compelling argument or vision is currently missing.

NATO also should better communicate the purpose and intent of its Enhanced Forward Presence units—battalion-sized infantry units now stationed in the Baltic states. Russia is seeking to drive a wedge between Russian-speaking populations in the region and these units. Public affairs elements attached to these units should help frame their presence and mission and tell their story with compelling social media content. Civil affairs activities can also be used to their advantage. For example, after U.S. soldiers helped cut firewood for local Russian speaking residents, one resident was heard saying, "Russian soldiers would never do that."

Highlight and "Tag" Russian Propaganda

The current approach to highlighting Russian propaganda is to do so through websites or email alerts. Unfortunately, such efforts are extremely slow, and the messages fail to reach the populations most in need. It is critical to highlight Russian propaganda in speedy ways that target the audiences at risk. Our study highlights the potential use of Google Ads. This approach uses videos and other content embedded in Google search results to educate populations who search for Russian-created fake news on Google and other search engines. The report also notes the potential value of viewpoint bots. A viewpoint bot can, in theory, use advanced algorithms to identify Russian bots or trolls engaged in hashtag campaigns. Once it identifies a bot or troll, the viewpoint bot posts messages to the offending hashtags, informing audiences of Russian influence efforts.

Build the Resilience of At-Risk Populations

In the Baltic states, we frequently heard of the need for media literacy training, and there is a growing recognition of the need for such training in general. Facebook has begun broad-based media literacy training, and several countries, including Canada, Australia, and Sweden, now introduce media literacy training into their education system. While this is a long-term solution, such efforts would likely be warranted in the Baltic states and Ukraine. In the short term, there may be value in launching a public information campaign that can more immediately convey the concepts of media literacy and the risk of Russian propaganda to a mass audience.

Track Russian Media and Develop Analytic Methods

For the United States, allied governments, and technology firms to take any action against Russian social media operations, it will be critical to identify Russian bot and troll accounts and track their activity in real time. This is no small problem, as such accounts can be very difficult for the naked eye or even computer algorithms to spot. It will be critical to develop advanced computational analytics that can distinguish between authentic social media chatter and adversarial information campaigns. This will require a coordinated research program.

Chairman BURR. Thank you, Dr. Helmus.
Ms. DiResta.

STATEMENT OF RENEE DiRESTA, DIRECTOR OF RESEARCH, NEW KNOWLEDGE

Ms. DIRESTA. Thank you, Chairman, Vice Chairman and members of the Committee, for giving me the opportunity to address this body today. I'm Renee DiResta, Director of Research at New Knowledge, and I study computation propaganda.

Disinformation, misinformation and social media hoaxes have evolved from a nuisance into a high-stakes information war. Our frameworks for dealing with them have not evolved. We discuss counter-messaging, treating this as a problem of false stories rather than as an attack on our information ecosystem.

We're in the midst of an arms race, in which responsibility for the integrity of public discourse is largely in the hands of private social platforms, and determined adversaries continually find new ways to manipulate features and circumvent security measures. Computational propaganda and disinformation is not about arbitrating truth, nor is it a question of free speech. It's information warfare, it's a cybersecurity issue, and it must be addressed through collaboration between governments responsible for the safety of their citizens and private industry responsible for the integrity of their platforms.

Malign narratives have existed for a very long time, but today's influence operations are materially different because the propaganda is shared by friends on popular social platforms. It's efficiently amplified by algorithms, so campaigns achieve unprecedented scale. Adversaries leverage the entire information ecosystem to manufacture the appearance of popular consensus. Content is created, tested and hosted on platforms such as YouTube, Reddit and Pinterest; it's pushed to Twitter and Facebook with their standing audiences in the hundreds of millions, and it's targeted at the most receptive.

Trending algorithms are gamed to make content go viral. This often has the added benefit of mainstream media coverage on traditional channels, including television. And if an operation is successful and the content gets wide distribution, recommendation and search engines will continue to serve it up.

We're here because the Internet Research Agency employed this playbook. Their operation began around 2013, continued throughout the 2016 election, and even increased on some platforms, such as Instagram and Twitter, in 2017. The operation reached hundreds of millions of users across Facebook, Twitter, Vine, YouTube, G+, Reddit, Tumblr, and Medium. Websites were created to push content about everything from social issues to concerns about war, the environment and GMOs.

Twitter accounts masqueraded as local news stations, WhiteHouse.gov petitions were co-opted, Facebook events were promoted, and activists were contacted personally via Messenger to take the operation to the streets. Twitter accounts and Facebook accounts associated with the IRA remain active today.

The focus of the IRA campaign was to exploit social and especially racial tension. Despite YouTube's claim that the content

found on its platform was not targeted to any particular sector of the U.S. population, the majority was related to issues of importance to the black community, particularly officer-involved shootings. Hundreds of thousands of Americans liked Facebook pages with names like Blacktivist, Heart of Texas and Stop All Invaders.

The amount of explicitly political content that mentioned the candidates in 2016 was small, but unified in its negativity towards the candidacy of Secretary Clinton. In content that targeted the left, this included messages aimed at depressing the turnout, particularly among black voters, or painting Secretary Clinton in a negative light compared to Jill Stein or Bernie Sanders.

Only the social networks that hosted this campaign are currently in a position to gauge its impact.

The IRA was not the only adversary to target American citizens online. The co-opting of social networks reached mainstream awareness in 2014, as ISIS established a virtual caliphate across all social platforms.

The debate about what to do about that made it obvious that no one was in charge. That confusion continues even as the threat expands. The Wall Street Journal recently revealed that a private intelligence company, Psy-Group, marketed their ability to conduct similar types of influence operations to impact the 2016 election.

Social platforms have begun to take steps to reduce the spread of disinformation and deserve credit for doing that. These steps, several of which were inspired by prior hearings in this chamber, are a good start, but as platform, tactics and protections change, determined adversaries will develop new tactics.

We should anticipate an increase in the misuse of less resourced social platforms. We should anticipate an increase in the use of peer-to-peer encrypted messaging services. Future campaigns will likely be compounded by the use of witting or unwitting persons through whom state actors will filter their propaganda. We anticipate the incorporation of new technologies, such as video and audio produced by AI, to supplement these operations, making it increasingly difficult for people to trust what they see.

This problem is one of the defining threats of our generation. Influence operations exploit divisions in our society using vulnerabilities in our information ecosystem. They take advantage of our commitment to freedom of speech and the free flow of ideas. The social media platforms cannot and should not be the sole defenders of democracy and public discourse.

So, we recommend immediate action to identify and eliminate maligned influence campaigns and to educate the public in preparation for the 2018 elections. We recommend an updated global IO doctrine, including a clear delegation of responsibility within the U.S. government. We believe that private tech platforms must be held accountable to ensure that they're doing their utmost to mitigate the problem in our privately owned public squares, and oversight is key.

Finally, we need structures and cooperation, information-sharing between the public and private sectors. Formal partnerships between security companies, researchers and the government will be essential to defending our values, our democracy and our society.

In closing, thank you for the opportunity to participate in this conversation.

[The prepared statement of Ms. DiResta follows:]

Statement for the record from Renee DiResta, Director of Research, New Knowledge

Honorable Committee Members –

My name is Renee DiResta, and I research influence operations and social network manipulation. I appreciate the opportunity to submit this written and verbal testimony to your committee.

Over the past decade, disinformation, misinformation, and social media hoaxes have evolved from a nuisance into high-stakes information war. Our frameworks for dealing with them, however, remain the same -- we discuss counter-messaging and counter-narratives, falling into the trap of treating this as a problem of false stories rather than as an attack on our information ecosystem. We find ourselves in the midst of an arms race, in which responsibility for the integrity of public discourse is largely in the hands of private social platforms, and determined adversaries continually find new ways to manipulate evolving feature sets and circumvent new security measures. It is critical to acknowledge that computational propaganda and disinformation is not about arbitrating truth, nor is it a question of free speech. Information Warfare is a cybersecurity issue, it is an ongoing national security issue, and it must be addressed through a collaboration between governments responsible for the safety of their citizens and private industry responsible for the integrity of their products and platforms.

Propaganda and malign narratives have existed for a very long time, but today's influence operations, which co-opt popular social platforms, are materially different – the propaganda is shared by our friends, often in the form of highly effective, shareable, immediately graspable memes. It is efficiently amplified by algorithms, and the campaigns achieve unprecedented scale. To conduct an operation, adversaries leverage the entire media ecosystem to push a narrative and manufacture the appearance of popular consensus. The operation is planned on one platform, such as a messaging or chat board. Content is created, tested, and hosted on others, such as Reddit, Pinterest and YouTube. It's then pushed to platforms like Twitter and Facebook, with standing audiences of hundreds of millions of people, and targeted at those most likely to be receptive to it. The platform's trending algorithms are gamed to make the content go viral - this often delivers the added benefit of mainstream media coverage, increasing attention via traditional media channels including television. If an operation is successful and the content gets wide distribution, or a manipulative Page or Group gains enough followers, the recommendation engine and search engine will continue to

serve up the content on an ongoing basis.

We are here because the Internet Research Agency (IRA) employed this playbook, conducting an operation that leveraged our social networks to spread propaganda and disinformation directly to American citizens. Their operation likely began sometime in 2013, continued throughout the 2016 election cycle, and even increased on Instagram in 2017. While many accounts were shut down in 2017 as the tech companies began their investigations, Twitter accounts and Facebook pages associated with the IRA remain active. The IRA content on Facebook and Instagram alone had 293 million engagements; Facebook itself estimates 146 million users across the two platforms were affected. The Internet Research Agency's disinformation campaign was conducted on all the major platforms in the social network ecosystem. The presence of manipulated content on Facebook and Twitter is well-documented. In the case of Alphabet, YouTube, G+, Gmail, and Google Voice were all leveraged to either host content or to support personas. Reddit, Tumblr, and Medium have confirmed that they were misused; Twitter's Vine video app was co-opted as well, and IRA meme boards were discovered on Pinterest. Games and music apps were created and pushed to teenagers to download. Even popular game Pokemon Go was incorporated into the operation. Outside of social platforms, a number of websites were created to host original written content, many of which looked very much like citizen journalism-style blogs and think tanks. Topics ran the gamut, from social issues to concerns about wars, the environment, corporate greed, GMOs, energy policy, and immigration. Twitter accounts were created to masquerade as local news stations. White House petitions were either created or co-opted to engineer a perception of social consensus. Dozens of Facebook Events were promoted, and activists were contacted personally via Messenger, to take the operation to the streets.

The Internet Research Agency's campaign pressed on a variety of socially divisive issues, but the primary focus was on racial tension. Despite YouTube's claim that the content attributed to the IRA on its platform was "not targeted to the US or to any particular sector of the US population", it appears that the overwhelming majority of the videos were related to issues of importance to the black community, particularly officer-involved shootings. Hundreds of thousands of Americans liked Facebook Pages with names like Blacktivist, Heart of Texas, and Stop All Invaders. The percentage of explicitly political content that mentioned candidates by name was small – approximately 10% – but the political content targeting both right-leaning and left-leaning Americans was unified in its negativity toward the candidacy of Secretary Clinton. In pages targeting the left, this included content intended to depress voter

turnout among black voters, or to paint Secretary Clinton in a negative light as compared to candidates Jill Stein or Senator Bernie Sanders. Only the social networks that hosted this campaign are in a position to gauge its full impact in changing voter attitudes on their respective platforms. However, independent of its impact, the fact that it was attempted, went undetected, and achieved such significant reach is sufficient cause for concern.

Although this hearing was convened because of the Internet Research Agency's interference in the 2016 election, Russia was not the first to target American citizens with propaganda using the social ecosystem. In 2014, the co-opting of social communication infrastructure rose to mainstream awareness in the United States as ISIS established a virtual caliphate, using every social app imaginable to push propaganda boldly and transparently, using the features of our of social ecosystem in precisely the way they were meant to be used: to build an audience and connect with followers. This was a visible indication that the tools built to enable marketers and messengers and friends to communicate could be co-opted and misused; the ensuing debate about what to do about the problem made it apparent to anyone watching that no one was in charge, and that American companies, American civil society organizations, and the American government were deeply divided on how to respond to the threat. That confusion continues even as the threat expands beyond extremists and state actors: the Wall Street Journal recently revealed that a private intelligence company, Psy-Group, openly marketed their ability to conduct similar types of influence operations to impact the 2016 election.

As the internet has evolved, we've seen the consolidation of users into large standing audiences on a small handful of social networks. This infrastructure has been a phenomenal tool for small businesses to reach customers, and for the previously voiceless to find a voice. But like any tool without appropriate safeguards, it can be misused. These platforms employ gameable algorithms, and facilitate personalized targeting that is enabled by the ongoing collection of extensive amounts of personal data. As a result, social networks continue to be the most effective vector to manipulate public sentiment and cause lasting damage to our democratic process. To combat this evolving threat, we have to address those structural weaknesses and design an effective deterrence strategy.

Individually, several social platforms have begun to take steps to reduce the spread of disinformation, by disrupting economic incentive structures, reducing the spread of

clickbait headlines, and reducing the granularity of targeting criteria that were used to push malicious content directly to subsets of the American people. Political ad content on Facebook and Twitter is somewhat public now; we look forward to this database being searchable via API, better equipping researchers and journalists to understand our paid political conversation. Several platforms are beginning to take source quality into account, which may help curb the ability of manipulative propaganda websites to reach their audience. These steps, several of which were inspired by prior hearings in this chamber, are a good start. But as platform features and protections change, determined adversaries will develop new tactics.

In addition to the ongoing exploitation of social divisions, targeting of elections, and disinformation about geopolitical events (such as the conflict in Syria), campaigns targeting U.S. industry have emerged and are thriving. Influence operations are increasingly appealing to a variety of actors: ideological true believers, non-state extremists, economically-motivated enterprises, and State Actors. The last of these requires a whole-of-government defense strategy, as it's unlikely that commercial platforms will be able to compete with the sophistication of well-resourced and motivated hostile foreign government experienced in bypassing common security checks.

The gaps in our ability to combat this type of information warfare became apparent while attempting to address ISIS propaganda: the U.S. government was legally constrained in its ability to respond, and the social platforms proved slow to act as extremist content, assisted by platform targeting algorithms, easily made its way into the social feeds of Americans. That wake-up call fell on deaf ears as our adversaries prioritized, deployed, and perfected their influence operation capabilities. They were able to exploit gaps in our intelligence community's authorities, and take advantage of our commitment to civil liberties; this left social platforms in the impossible position of having to individually respond to this global threat, which has resulted in the implementation of inadequate solutions and self-serving defensive policies on the part of those private companies.

Several years after the threat emerged, the U.S. Government and the tech industry respectively took small steps towards combating this threat by establishing the Global Engagement Center and the Global Internet Forum to Counter Terrorism. The focus of the latter is still solely terrorism, although the Global Engagement Center's mandate has expanded to countering foreign propaganda. The DOJ and NSA & Cyber Command's

recent announcements that they will prioritize the mitigation and prosecution of this activity is a positive sign. However, addressing this asymmetric threat requires a 21st century Information Operations Doctrine, the implementation of a global real-time detection and deterrence strategy, and the cooperation of private industry, press, law enforcement, and the intelligence community.

The evolution of social media propaganda and influence techniques will bring serious threats. We should anticipate an increase in the misuse of less popular and less resourced social platforms, and an increase in the use of peer-to-peer messaging services. We believe that future campaigns will be compounded by the employment of witting or unwitting U.S. Persons through whom these state actors will filter their propaganda, in order to circumvent detection by social platforms and law enforcement. We should anticipate the incorporation of new technologies, such as videos and audio produced by artificial intelligence, to supplement these operations, making it increasingly difficult for citizens to trust their own eyes.

This will be one of the defining threats of our generation. Influence operations exploit divisions in our society using vulnerabilities in our information ecosystem. They take advantage of America's commitment to freedom of speech and the free flow of ideas. The social media platforms cannot, and should not, be the sole defenders of democracy and public discourse. In that light, here are several recommendations we are proposing toward achieving the goal of restoring integrity to the information ecosystem:

First, to address the most pressing short term issue, we recommend immediate government action to identify and eliminate malign influence campaigns and to educate the public in preparation for the 2018 elections.

Second, this domestic defense must be complimented by an updated global IO doctrine and international detection and deterrence strategy, with the goal of mitigating foreign influence targeting our allies, including the clear delegation of responsibility of this activity within the U.S. Government. Taking example from the U.S. Government's cyber security response over the past decade, we must implement legislation that defines and criminalizes foreign propaganda that targets not just our political process but also addresses the targeting of commercial industry and social issues. Empowering law enforcement with updated legal tools to investigate and prosecute sophisticated foreign propaganda is essential to combatting this threat in the age of information warfare.

Third, the private tech platforms must be held accountable to ensure that they are doing

their utmost to manage and mitigate the pervasiveness of disinformation and manipulative narratives in our privately-owned public squares. A number of regulatory frameworks are on the table, including mandating that automated accounts be labeled, limiting high-frequency advertising practices, and curtailing and reporting inauthentic accounts. Regardless of which is chosen, and whether these policies are implemented voluntarily by platforms (self-regulatory action) or via formal regulation, the incorporation of oversight is key.

Finally, given that this asymmetric persistent threat impacts our social, geo-political, and economic spheres, and given the sophistication of its tradecraft, we need new structures for cooperation and information sharing between the public and private sectors. Formal partnerships between security companies, researchers, and government will be essential to defending our values, our democracy, and our society.

Thank you.

Chairman BURR. Thank you, Ms. DiResta.
Dr. Kelly.

STATEMENT OF JOHN W. KELLY, Ph.D., FOUNDER AND CEO, GRAPHIKA

Dr. KELLY. Chairman Burr, Vice Chairman Warner, members of the Committee: Thank you for this opportunity to appear before you today to discuss the weaponization of our social media platforms and the resulting harm to our democracy.

The data now available make it clear that Russian efforts are not directed against one election, one party, or even one country. We are facing a sustained campaign of organized manipulation, a coordinated attack on the trust we place in our institutions and in our media, both social and traditional.

These attacks are sophisticated and complex, and the Committee's bipartisan work to untangle and expose them sets a great example for the country.

I am a social scientist and the CEO of a marketing analytics firm that develops advanced techniques for understanding the flow of information online. My experience with Russian online communities began 10 years ago when I helped lead a research effort at Harvard's Berkman Klein Center for Internet & Society. In this work, we observed Russia's own online political discussion evolve from a vigorously free and open forum with a wide variety of organic voices and viewpoints to a network rife with automated accounts and organized pro-government trolling. In short, for the past several years the Russian government has been doing to us what they first did at home and in Eastern Europe a decade ago.

We know this because of indispensable work by a wide range of investigative journalists, academic researchers, NGOs, grassroots organizations, often conducted at great personal risk. For more than a decade, these groups have documented the playbook used by the Russian government to spread chaos and discord online. These techniques include crafting fictitious online personas to infiltrate communities, infiltrating radical political communities on both sides to enhance their mutual distrust, targeting both sides of a country's most divisive issues, mixing pop culture references and radical political discourse to influence young minds, using bots and trolls for inorganic amplification, launching cyberattacks in conjunction with information operations.

Again, each one of these features of the Russian government's attack against the American public was first tested and deployed against their own people, and then refined to target their chosen enemies abroad.

Thanks to the great work of this Committee and to the cooperation of social media platforms, data documenting the Internet Research Agency's U.S.-focused effort in 2016 has now been released to the public. Many dissertations will be written on this data, but today I want to highlight just three points.

First, Russian manipulation did not stop in 2016. After Election Day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election.

Second, they are targeting both sides of our political spectrum simultaneously, both before the 2016 election and right now. We see from the IRA data how the same Russian organization will use sophisticated false personas and automated amplification on the left and the right in an attempt to exploit an already divided political landscape.

Our current landscape is particularly vulnerable to these sorts of attacks. In our estimate, today the automated accounts at the far left and the far right extremes of the American political spectrum produce as many as 25 to 30 times the number of messages per day on average as genuine political accounts across the mainstream. The extremes are screaming while the majority whispers.

Third, American media is also being targeted. The IRA persona "Jenna Abrams," which had accounts on multiple platforms, was cited by over 40 U.S. journalists before being unmasked. The Russian activity seeks to turn the normal differences of opinion among Americans into headlines about unbridgeable political divisions. American journalism has a responsibility to harden itself to these manipulations.

The platform's proactive transparency in these matters will be critical in keeping us ahead of the new efforts and tactics and to informing public debate on how to strengthen our democracy in the face of these threats. There are significant challenges ahead of us, and, unfortunately, knowing the other team's playbook does not mean you are going to win the game.

The released data allow us to understand what the IRA did in retrospect. Detecting these efforts before they have already had their intended effect and agreeing on how to address them remains a formidable challenge.

On the technological front, our field is making progress in discerning technical markers that distinguish true grassroots movements from fabricated campaigns. And research is yielding methods for detecting manipulations before they gain momentum. It is equally important to keep our values front and center in this work, notably our dedication to freedom of expression and to protecting user privacy.

It will take skilled women and men professionally dedicated to this task and an investment in the development of tools and methods to first catch up and then stay ahead in our race to defend America's cyber social fabric from a new form of 21st-century warfare.

Civil society or media institutions in the technology sector can only do so much in the face of it. The responsibility also lies with government to ensure that any state actor eager to manipulate and harass faces consequences for their actions. It is not just bots that are attacking us and it's not just algorithms that must protect us.

The efforts of this Committee represent a tremendous step forward in what will undoubtedly be a long and challenging process, and I commend its leadership, dedication, thoroughness and bipartisan spirit.

Thank you again for the opportunity to participate today.

[The prepared statement of Dr. Kelly follows:]

Graphika

BRIEFING FOR THE UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE
Statement of Dr. John W. Kelly, Chief Executive Officer
Washington, DC
August 1, 2018

Chairman Burr, Vice Chairman Warner, members of the committee: Thank you for the opportunity to appear before you today to discuss the weaponization of our social media platforms and the resulting harm to our democracy.

The data now available make it clear that Russian efforts are not directed against one election, one party, or even one country. We are facing a sustained campaign of organized manipulation, a coordinated attack on the trust we place in our institutions and in our media - both social and traditional. These attacks are sophisticated and complex, and the committee's bi-partisan work to untangle and expose them sets a great example for the country.

I am a social scientist, and the CEO of a marketing analytics firm that develops advanced techniques for understanding the flow of information online. My experience with Russian online communities began ten years ago, when I helped lead a research effort at Harvard's Berkman-Klein Center for Internet & Society.[1] In this work, we observed Russia's own online political discussion evolve, from a vigorously free and open forum with a wide variety of organic voices and viewpoints, to a network rife with automated accounts and organized pro-government trolling.

In short, for the past several years, the Russian government has been doing to us what they first did at home and in Eastern Europe a decade ago.

We know this because of indispensable work by a wide range of investigative journalists, academic researchers, NGOs, and grassroots organizations, often conducted at great personal

---

[1] John Palfrey, Urs Gasser, John Kelly, Karina Alexanyan, Bruce Etling and Rob Faris (2010) *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, Berkman Klein Center for Internet & Society at Harvard University. Available here; Karina Alexanyan, Vladimir Barash, Bruce Etling, Rob Paris, John Palfrey, Urs Gasser, Hal Roberts and John Kelly (2012) *Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere*, Berkman Klein Center for Internet & Society at Harvard University. Available here.

risk. For more than a decade, these groups have documented[2] the playbook used by the Russian government to spread chaos and discord online. These techniques include:

- Crafting fictitious online personas to infiltrate communities
- Infiltrating radical political communities on both sides to enhance their mutual distrust
- Targeting both sides of a country's most divisive issues
- Mixing pop culture references and radical political discourse to influence young minds
- Using bots and trolls for inorganic amplification
- Launching cyber attacks in conjunction with information operations

Again, each one of these features of the Russian government's attack against the American public was first tested and deployed against their own people and then refined to target their chosen enemies abroad.[3]

Thanks to the great work of this committee and to the cooperation of social media platforms, data documenting the Internet Research Agency's US-focused effort in 2016 has now been released to the public. Many dissertations will be written on this data, but today I want to highlight just three points:

First, Russian manipulation did not stop in 2016.

After election day the Russian Government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election.

Second, they are targeting both sides of our political spectrum simultaneously, both before the 2016 election and right now.

We see from the IRA data how the same Russian organization will use sophisticated false personas and automated amplification, on the left and the right, in an attempt to exploit an already divided political landscape.[4] Our current landscape is particularly vulnerable to these sorts of attacks. In our estimate, today the automated accounts at the far left and far right extremes of the American political spectrum produce as many as 25 to 30 times the number of messages per day on average as genuine political accounts across the mainstream. The extremes are screaming while the majority whispers.

---

[2] *See for instance*: Ivan Sigal (13 October 2017) "Tracking Russian Online Interference Teaches Valuable Lessons on Improving News Quality." Global Voices. Available here.; Max Seddon (June 2, 2014) "Documents Show How Russia's Troll Army Hit America," Buzzfeed News. Available here; Adrian Chen (June 2 2015) "The Agency" New York Times. Available here; Leo G. Stewart, Ahmer Arif, and Kate Starbird. 2018. "Examining Trolls and Polarization with a Retweet Network." ACM, New York, NY, USA, 6 pages. Available here.

[3] Ellen Nakashima (December 25, 2017) "Inside a Russian disinformation campaign in Ukraine in 2014," Washington Post. Available here;

[4] Darren L. Linvill and Patrick L. Warren (2018) "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building," Clemson University. Working Paper available here.

Third, American media is also being targeted. The IRA persona "Jenna Abrams," which had accounts on multiple platforms, was cited by over 40 US journalists before being unmasked.[5] The Russian activity seeks to turn the normal differences of opinion among Americans into headlines about unbridgeable political divisions. American journalism has a responsibility to harden itself to these manipulations.

The platforms' proactive transparency in these matters will be critical to keeping us ahead of new efforts and tactics, and to informing public debate on how to strengthen our democracy in the face of these threats.

There are significant challenges ahead of us, and unfortunately, knowing the other team's playbook does not mean you are going to win the game. The released data allow us to understand what the IRA did in retrospect. Detecting these efforts before they have already had their intended effect - and agreeing on how to address them - remains a formidable challenge.

On the technological front, our field is making progress on discerning technical markers that distinguish true grassroots movements from fabricated campaigns, and research is yielding methods for detecting manipulations before they gain momentum. It is equally important to keep our values front and center in this work, notably our dedication to freedom of expression and to protecting user privacy.

It will take skilled women and men professionally dedicated to this task and an investment in the development of tools and methods to first catch up, and then stay ahead, in our race to defend America's cyber-social fabric from a new form of Twenty First Century warfare.

Civil society, our media institutions, and the technology sector can only do so much in the face of it: the responsibility also lies with Government to ensure that any state actor eager to manipulate and harass[6] faces consequences for their actions. It's not just bots that are attacking us, and it's not just algorithms that must protect us.

The efforts of this committee represent a tremendous step forward in what will undoubtedly be a long and challenging process, and I commend its leadership, dedication, thoroughness, and bipartisan spirit. Thank you again for the opportunity to participate today.

---

[5] Joseph Cox and Ben Collins (2 November 2017) "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World." The Daily Beast. Available here.

[6] *See for instance:* Michael Riley, Lauren Etter and Bibhudatta Pradhan (19 July 2018) "A Global Guide to State-Sponsored Trolling." Bloomberg. Available here; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." Working Paper 2018.1. Oxford, UK: Project on Computational Propaganda. Available here.

Chairman BURR. Thank you, Dr. Kelly.
Ms. Rosenberger.

STATEMENT OF LAURA ROSENBERGER, DIRECTOR, ALLIANCE FOR SECURING DEMOCRACY AT THE GERMAN MARSHALL FUND OF THE UNITED STATES

Ms. ROSENBERGER. Thank you, Chairman Burr, Vice Chairman Warner and distinguished members of the Committee. I submitted my full statement for the record, but let me highlight a few key points on the national security context of these activities and steps we need to take to address them.

The health and strength of our democracy depends on 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.

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

The 9/11 Commission characterized the failures that preceded that attack as a failure of imagination. I believe the failure to detect and disrupt the Russian government's weaponization of online platforms to be a similar failure to imagine, not just by the government but also by those who ought to understand these tools best, their creators.

Thanks in part to the bipartisan work of this Committee, we now know that Russian government-linked actors used a range of means to manipulate the online information space, using nearly every social media and online platform to amplify extreme content and promote polarization, manipulate search results, encourage action off-line, undermine faith in institutions, insinuate themselves to target audiences in order to influence public debates on geopolitics, and spread hacked information.

And, it's not just the Internet Research Agency. We know Russian military intelligence officers used fake social media personas and websites, and the United States is not the only target.

The Chinese government has also begun to use social media to manipulate conversation and public opinion outside of its borders. Our authoritarian adversaries are using these platforms because controlling the information space is a powerful means to undermine democratic institutions and alliances and advance their geopolitical goals. But meaningful actions to close off these vulnerabilities by both government and the private sector are lacking, and as we focus on the past we are missing what still is happening and what will happen again. What may have once been a failure to imagine is now a failure to act.

Fundamentally, this is not a content problem. This is a deliberate manipulation of the information space by actors with malicious intent engaging in deceptive behavior. Transparency and exposure of manipulation is critical to reducing its effectiveness and

deterring it, but tech companies have remained defensive and reluctant to share information. Their focus cannot be on public relations campaigns; it needs to be on detailing the nefarious activities these companies are seeing and curtailing it. Facebook's announcement yesterday is what we need more of.

Transparency is also critical for accountability, and outside researchers need greater access to data in a manner that protects users' privacy. Users also need more context about the origin of information and why they see it, including disclosure of automated accounts while protecting anonymity.

Identifying malicious actors and their patterns of activity requires new mechanisms for sharing data, both between the public and private sectors and among technology companies. Massive efforts along these lines are welcome, but need to be streamlined and institutionalized and protect privacy and speech.

We also need to identify threats in new technology before they are exploited. AI presents new tools to both combat the problem as well as new ways to make it worse, such as deep fakes. Government and tech companies need to close off vulnerabilities that are being exploited, including by providing a legal framework such as the Honest Ads Act that applies the same standards to political ads online that apply off-line.

Manipulation of social media is one part of a larger strategy to weaken our democracy. My bipartisan program recently released a policy blueprint for countering authoritarian interference in democracies endorsed by a bipartisan and trans-Atlantic group of former national security officials. Our recommendations include sending clear deterrent warnings to foreign actors about the consequences for such activity and identifying our own asymmetric advantages.

Government also needs to expose foreign interference publicly, and legislating reporting requirements for the Executive Branch would ensure that politics are not a consideration.

We also need to harden our electoral infrastructures through measures like the Secure Elections Act, as cyber attacks remain a core part of Moscow's arsenal. More broadly, the government needs a unified and integrated approach, including through a counter-foreign-interference coordinator at the National Security Council and a National Hybrid Threat Center.

Finally, this is a transnational challenge and it is essential that we work more closely with allies and partners to share information about threats and collaborate on responses.

Distinguished members, there are steps that we can take today to make our democracy more secure. We need to come together 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. In the face of this threat, standing together as Americans has never been more important.

Thank you.

[The prepared statement of Ms. Rosenberger follows:]

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?EzqGtMwOAjQIIH8eRNNoZ10T49OV63Ih.

[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.

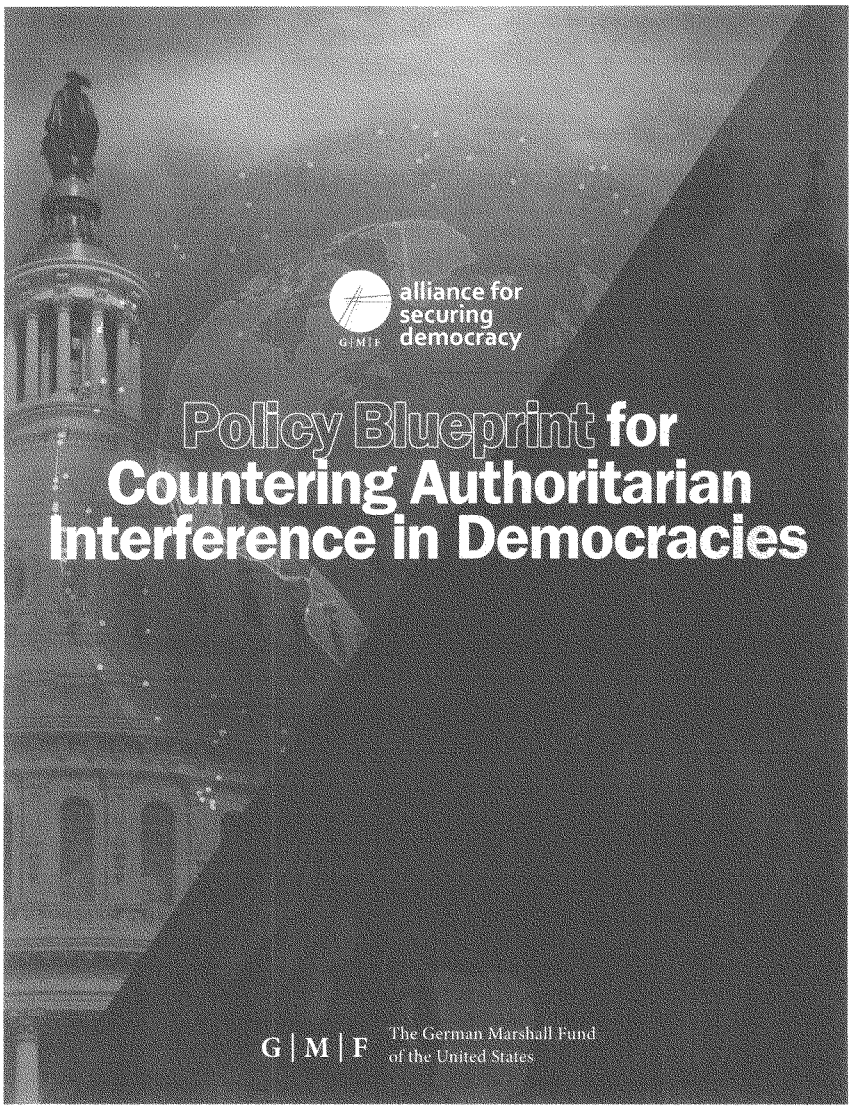
[44] Leaders of the Group of Seven, "Charlevoix Commitment on Defending Democracy from Foreign Threats," June 9, 2018, https://g7.gc.ca/wp-content/uploads/2018/06/DefendingDemocracyFromForeignThreats.pdf.

[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


alliance for
securing
democracy
GMF
Policy Blueprint for
Countering Authoritarian
Interference in Democracies
G | M | F
The German Marshall Fund
of the United States

45

POLICY BLUEPRINT FOR COUNTERING AUTHORITARIAN INTERFERENCE IN DEMOCRACIES

2018 | No.27

JAMIE FLY, LAURA ROSENBERGER, AND DAVID SALVO

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@securingdemocracy.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

About the Authors

Jamie Fly is a senior fellow and director of the Future of Geopolitics and Asia programs at The German Marshall Fund of the United States.

Laura Rosenberger is the director of the Alliance for Securing Democracy and a senior fellow at The German Marshall Fund of the United States (GMF)

David Salvo is the deputy director of the Alliance for Securing Democracy

About the Alliance for Securing Democracy

The Alliance for Securing Democracy is a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States (GMF) that is committed to developing comprehensive strategies to defend against, deter, and raise the costs on Russian and other state actors' efforts to undermine democracy and democratic institutions. The Alliance is informed by a bipartisan, transatlantic advisory council composed of former senior officials with experience in politics, foreign policy, intelligence, Russia, and Europe — bringing deep expertise across a range of issues and political perspectives.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

Photo Credits: Unsplash.com/ Shutterstock.com

Executive Summary

In 2014, Russian government operatives began attacking American democracy through a multifaceted operation, a campaign that followed years of similar activity across Europe. A core component of this operation was the Russian government's aggressive interference in the 2016 presidential election, according to the unanimous conclusion of the U.S. intelligence community. Special Counsel Robert Mueller's February 16 indictment of the Internet Research Agency and related individuals, as well as the Senate Select Committee on Intelligence investigation, provided further details on the extent of Russia's interference in American democracy. Through e-mail hacks and leaks of information on politicians and campaigns, cyber-attacks against U.S. electoral infrastructure, and the injection of inflammatory material into the U.S. political and social ecosystems, the Kremlin sought to undermine the integrity of democratic institutions and amplify growing social and political polarization within and between the left and right. This campaign sought to damage Hillary Clinton's presidential campaign and boost Donald Trump's profile during the election. It also targeted prominent members of both parties, including members of the Trump administration, and average American citizens through political ads and disinformation on social media, a trend that continues to this day.

The Kremlin's operation to undermine democracy weaponized our openness as a nation, attempting to turn our greatest strength into a weakness, and exploited several operational and institutional vulnerabilities in American government and society:

- A government that was — and remains — unprepared to address asymmetric threats of this nature;
- Insufficient cyber defenses and outdated electoral infrastructure;
- Tech companies that failed to anticipate how their platforms could be manipulated and poor cooperation between the public and private sector to address technological threats;
- A highly polarized media environment which amplified Russian disinformation without regard for the credibility of the information they reported or the ethics of doing so;
- A porous financial system that allowed dirty or anonymous money to enter the country and facilitate the aims of corrupt foreign elite;
- The polarization of American citizens and the American political system; and,
- A general decline of faith in democracy and the media.

The Kremlin's playbook takes advantage of vulnerabilities and weaknesses in the societies it targets. In the United States, the vulnerabilities that the Kremlin exploited included operational and structural weaknesses in governance, legislation, and corporate policy. But they also exploited existing institutional and societal shortcomings in America. A hyper-partisan climate, declining faith in the ability of government to do its job, festering racial divisions, growing economic disparities, and the increasingly polarized media environment and prevalence of echo chambers, all provide fertile ground for adversaries who seek to do America harm. Addressing the threat of foreign interference requires closing both sets of vulnerabilities.

The tools the Kremlin has used to wage these operations include information operations, cyber-attacks, malign financial influence, support for political parties and advocacy groups, and state economic coercion. In a world increasingly interconnected by technology, state and non-state actors alike will be able to conduct malign interference operations of varying scales and sophistication. Other authoritarian regimes, such as China, have already adopted and begun to deploy asymmetric tools for their own interference operations. Some U.S. partners like Qatar and the United Arab Emirates are now even adopting similar tools as they attempt to influence American debates. As other foreign actors enter the field and as technology continues to rapidly advance, Western institutions, such as the EU and NATO, and democracies worldwide will face additional challenges.

A New Strategic Approach for Government and Society

Successive U.S. administrations of both parties neglected a threat once thought by many to be confined to Russia's periphery and not seen as a direct threat to U.S. national security. Tackling this challenge requires a new strategic approach for government and society to defend democracy against malign foreign interference, one that puts the problem at the forefront of the U.S. national security agenda and brings the public and private sectors together to complement each other's efforts. Rather than emulating the tactics used against us by authoritarian regimes, our responses should play to our strengths and be rooted in democratic values — respect for human and civil rights, including freedom of speech and expression and the right to privacy.

There must be a bipartisan response by the Executive Branch and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us. Defending against and deterring the threat also requires greater transatlantic cooperation at NATO and between the United States and the EU. Finally, Americans must rise above the polarization and hyper-partisanship in our media and civic discourse that exacerbated social and political divisions the Russian government exploited.

This report, representing the consensus of the Alliance for Securing Democracy's Advisory Council, a bipartisan, transatlantic group of national security experts, makes recommendations not only to government, but also to the various pillars of democratic society — civil society organizations, the private sector, including the tech companies, and media organizations — that all have important roles to play in defending democracies from foreign interference.[1] The report also outlines the asymmetric tools and tactics that authoritarian regimes use to undermine democracy, the types of influence operations that have been conducted across the transatlantic space over the past two decades, and the overall strategic approach that government and society should adopt in order to protect our democratic institutions from malign foreign influence.

Recommendations

The effort to tackle the authoritarian interference challenge will need to be as expansive and sustained as the threat, but there are immediate actions that Congress, government, and non-government actors can begin immediately:

1. Raise the cost of conducting malign influence operations against the United States and its allies.

The U.S. government at the highest level should publicly articulate a declaratory policy that makes clear it considers malign foreign influence operations a national security threat and will respond to them accordingly. The Executive Branch and Congress should also impose a broader set of sanctions and reputational costs against individuals and entities that conduct these operations, facilitate corruption, and support authoritarian regimes' destabilizing foreign policy actions. The Executive Branch should also employ cyber responses as appropriate to respond to cyber-attacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats. Authoritarians that attempt to interfere in democracies' domestic politics must know that the repercussions for doing so will be severe and sustained.

2. Close vulnerabilities that foreign adversaries exploit to undermine democratic institutions.

From conducting cyberattacks against outdated electoral infrastructure to exploiting legislative loopholes to move money into the United States for covert political influence, foreign actors take advantage of our weaknesses in government. The administration and Congress should take several steps to ensure the integrity of our electoral process ahead of the 2018 midterm elections, as well as the integrity of our political system by closing off illicit finance and covert political influence from abroad. Government should also organize itself to respond to these threats more effectively by appointing a

1 The members of the Advisory Council of the Alliance for Securing Democracy endorse this report, indicating their support for its goals, direction, and judgments. Endorsement does not necessarily denote approval of every finding and recommendation. Advisory Council members contribute to the Alliance for Securing Democracy in their individual capacities.

senior-level Foreign Interference Coordinator ideally at the level of Deputy Assistant to the President at the National Security Council and establish a Hybrid Threat Center at the Office of the Director of National Intelligence to coordinate policy and intelligence across the U.S. government respectively.

3. Separate politics from efforts to unmask and respond to foreign operations against the U.S. electoral process. An incumbent government must be able to respond to an attack on our electoral system without being susceptible to accusations of political machinations. Congress should institute mandatory reporting requirements so that an administration must inform lawmakers of foreign attacks against U.S. electoral infrastructure, including individual political campaigns. Political parties and candidates running for office should also pledge publicly not to use weaponized information obtained through hacks or other illicit means.

4. Strengthen partnerships with Europe to improve the transatlantic response to this transnational threat.

Through bilateral relationships, cooperation with the EU and at NATO, and coordination between NATO and the EU, the United States and Europe can do a lot together to better defend and deter foreign influence operations: strengthen the sanctions regime on both sides of the Atlantic; shut down channels of money laundering and other forms of illicit finance; improve NATO's capabilities to support allies in responding to foreign influence operations; and, increase assistance to civil society within EU member states and in the surrounding neighborhood. The transatlantic community, together with democratic allies and partners worldwide, should establish a coalition to defend democracies to share information, analysis, and best practices to combat malign foreign influence operations.

5. Make transparency the norm in the tech sector.

Tech companies have released some data about the manipulation of their platforms by foreign actors, but the entire tech sector needs to be more proactive in providing Congress and the public information about their technology, privacy policies, and business models. Tech companies should also be more open to facilitating third-party research designed to assist them in defending their platforms from disinformation campaigns and cyber-attacks. Congress should help foster a culture of transparency, for example by passing legislation that ensures Americans know the sources of online political ads. Congress should also ensure that Americans' personal information is protected on social media platforms.

6. Build a more constructive public-private partnership to identify and address emerging tech threats.

The tech sector, the Executive Branch, and Congress need to establish a more constructive relationship to share information and prevent emerging technologies from being exploited by foreign adversaries and cyber criminals. New technologies, such as "deep fake" audio and video doctoring, will make the next wave of disinformation even harder to detect and deter. Platform companies need to collaborate more proactively with each other and with the U.S. government to mitigate threats that undermine democratic institutions.

7. Exhibit caution when reporting on leaked information and using social media accounts as journalism sources. As we witnessed throughout the 2016 presidential campaign, hacking operations by states and non-state actors are now a feature of political life in the democratic world. But the actors behind the hacks have an agenda, and that agenda can be enabled if media are not careful about how they report the story. Media organizations should also establish guidelines for using social media accounts as sources to guard against quoting falsified accounts or state-sponsored disinformation.

8. Increase support for local and independent media.

Today's media environment is dominated by the cable news networks, and, to a lesser extent, the major papers. Local and independent media are dying. That is bad for a number of reasons, including the fact that local media are often trusted to a greater degree than the major national news outlets. Philanthropic individuals and foundations

should support local journalism, as well as initiatives devoted to countering falsehoods propagated by foreign actors.

9. Extend the dialogue about foreign interference in democracies beyond Washington.

Government should help raise awareness about the threat of foreign interference, as exposure is one of the most effective means to building resilience and combating foreign interference operations. However, it should also seek partners in civil society who can combat foreign disinformation and effectively message to American and foreign audiences, and who are devoted to strengthening democratic values worldwide. New initiatives should be established to bring together civil society organizations to strengthen democratic institutions and processes in the United States. Washington-based officials and experts should also engage with Americans outside the Beltway more often to give them the tools they need to distinguish fact from fiction; identify trusted voices in local communities to participate in crafting solutions; and, foster a less politicized civic dialogue.

10. Remember that our democracy is only as strong as we make it.

The polarization of American society, reflected in our politics, contributed to the conditions that the Russian government exploited. All Americans have a responsibility to strengthen our democracy and address our problems at home that malign foreign actors use against us. Improving governance, strengthening the rule of law, fighting corruption, and promoting media literacy will help in this regard. Moreover, we need to instill a healthier respect for one another, regardless of our differences, by improving our civic discourse, practicing more responsible behavior on social media, respecting the vital role of the media, and calling on our elected officials to take action to defend our democracy on a bipartisan basis.

Foreward

"Nothing was more to be desired than that every practicable obstacle should be opposed to cabal, intrigue, and corruption. These most deadly adversaries of republican government might naturally have been expected to make their approaches from more than one querter, but chiefly from the desire in foreign powers to gain an improper ascendant in our councils. How could they better gratify this, than by raising a creature of their own to the chief magistracy of the Union?" –Alexander Hamilton, writing as "Publius," Federalist 68, March 14, 1788[2]

In May 2016, two groups of protestors faced each other in downtown Houston, Texas. One side was drawn there by a Facebook group called "Heart of Texas" to oppose the purported "Islamification of Texas." The other side was recruited by a Facebook group called "United Muslims of America" and was there to rally for "saving Islamic knowledge." The dueling protests in Houston led to confrontation and verbal attacks between the sides. What neither the protestors nor the authorities understood at the time was that both Facebook groups that spurred the protests were established and operated not by Houstonians, but by individuals posing as Americans from thousands of miles away. For relatively little cost, the Internet Research Agency (IRA), the now infamous troll farm in St. Petersburg, Russia, manipulated the most widely used social media platform to pit Americans in the United States' fourth-largest city against one another. The goal may have been to incite violence between these opposing groups of protestors. That outcome was thankfully avoided due to the presence of local law enforcement.[3]

Fast forward to fall 2017. Across the United States, NFL players were taking a knee during the playing of the national anthem to protest racial inequality and police brutality. On social media, a debate raged between Americans regarding whether the protesting players were disrespecting their flag and their country. Once again, Russian-linked accounts on social media fanned the flames and promoted conspiracy theories.[4] The Alliance for Securing Democracy's (ASD) Hamilton 68 Dashboard noticed a spike in activity from the Russian-linked accounts it tracks weighing in on behalf of both sides of the debate.[5] Over the past ten months, the Dashboard picked up similar trends during the protests in Charlottesville, Virginia over the removal of monuments to Confederate leaders, the "Me Too" movement to end sexual harassment and violence, debates about health care, and other hot-button social and political issues in the United States.

These events did not occur in isolation. They were part of a large-scale campaign run over the past several years by the Russian government and its proxies to undermine U.S. democracy and destabilize American society — following a pattern of similar activity to undermine democracies across Europe and weaken the transatlantic community for over a decade. More than a year and a half after the 2016 presidential election, this destabilization campaign continues.

The core component of this operation was the Russian government's aggressive interference in that election, according to the unanimous conclusion of the U.S. intelligence community.[6] Special Counsel Robert Mueller's February 16, 2018 indictment[7] of the IRA and related individuals, as well as the Senate Select Committee on Intelligence investigation[8], provided further details on the extent of Russia's attempted interference in our democratic institutions and society. The intelligence community continues to assess that Russia possesses the capabilities and intentions to interfere in future elections, a claim supported by senior members of President Donald

2 Alexander Hamilton, *The Federalist Papers*, No. 68, http://avalon.law.yale.edu/18th_century/fed68.asp.

3 Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," *The New York Times, February 18, 2018*, https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html.

4 Donie O'Sullivan, "American Media Keeps Falling for Russian Trolls," *CNNTech, June 21, 2018*, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

5 "Hamilton 68: Tracking Russian Influence Operations on Twitter," *Alliance for Securing Democracy*, https://dashboard.securingdemocracy.org/.

6 "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

7 U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," February 16, 2018, https://www.justice.gov/file/1035477/download.

8 U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

Trump's administration, notably Secretary of State Mike Pompeo[9] and Director of National Intelligence Dan Coats.[10]

The Kremlin's playbook takes advantage of vulnerabilities and weaknesses in the societies it targets. In the United States, the vulnerabilities that the Kremlin exploited included operational and structural weaknesses in governance, legislation, and corporate policy. But they also exploited existing institutional and societal shortcomings in America. A hyper-partisan climate, declining faith in the ability of government to do its job, festering racial divisions, growing economic disparities, and the increasingly polarized media environment and prevalence of echo chambers, all provide fertile ground for adversaries who seek to do America harm. Addressing the threat of foreign interference requires closing both sets of vulnerabilities. The threat of foreign interference is one of several threats to our national security and democracy, but part of reducing its potency must be addressing the underlying conditions at home that allow these tactics to succeed.

Russia's actions to undermine U.S. democracy should serve as a wake-up call to all Americans. Our freedoms are preserved by a democratic system that is built upon free and open debate and the institutions that protect the rights that make such debate possible. Now our freedom and openness are being used by authoritarian adversaries of the United States to attempt to undermine our unity and ultimately our power and ability to engage in the world. We must learn the lessons of 2016 and address the institutional failures that led to the first significant foreign interference in an American election in the modern era.

> ***"It is important to address the challenge to our democracy through bipartisan efforts by the administration and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us."***

This is not a question of the legitimacy of the 2016 election outcome. Ongoing investigations into the election should be allowed to run their course and routine congressional oversight of the Executive Branch must continue. Debates about the presidency of Donald Trump will continue to divide Americans. Yet what should unite Americans is the fact that Russia interfered in the U.S. election and continues to attempt to undermine the core of what makes us American — our democratic institutions. Left unaddressed, this threat will only grow as other authoritarians adopt similar tactics and use new technologies to make the threat even more persistent and potentially damaging. A divided response to Russia's interference plays into Vladimir Putin's hands and ensures that the Kremlin's original interference effort is successful.

That is why it is so important to address this challenge to our democracy through *bipartisan* efforts by the administration and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us. Rather than emulating the tactics used against us by authoritarian regimes, our responses should play to our strengths and be rooted in democratic values — respect for human and civil rights, including freedom of speech and expression and the right to privacy.

This report, representing the consensus of the Alliance for Securing Democracy's Advisory Council, a bipartisan, transatlantic group of national security experts, makes recommendations not only to government, but also to those that uphold the pillars of democratic society — civil society organizations, the private sector, including the tech companies, media organizations, and ultimately our fellow citizens — who all have important roles to play in defending democracies from malign foreign

9 Cristiano Lima, "Pompeo: 'I Have Every Expectation' Russia Will Meddle in 2018 Elections," *Politico*, January 30, 2018, https://www.politico.com/story/2018/01/30/russia-2018-election-meddling-376826.

10 Kevin Johnson, "'The United States Is Under Attack': Intelligence Chief Dan Coats Says Putin Targeting 2018 Elections," *USA Today*, February 13, 2018, https://www.usatoday.com/story/news/politics/2018/02/13/intelligence-director-coats-says-u-s-under-attack-putin-targeting-2018-elections/332566002/.

influence operations.[11] The report also outlines the tools and tactics that authoritarian regimes use to undermine democracy and the broader context of influence operations across the transatlantic space over the past two decades, of which the operation against the United States was only one of the most recent. It recommends a new strategic approach that government and society should adopt to protect our democratic institutions from authoritarian interference.

I. The Operation against America

How the Kremlin Interfered in the U.S. Election and Targeted American Political Debates

When the Kremlin launched its operation against the United States in earnest in 2014, it did not start with an emphasis on a particular candidate for office. Instead, it adapted tactics out of the Soviet playbook. During the Cold War, the Soviet Union used so-called "active measures," to attempt to exploit divisions in American society. In its modern incarnation, the Russian government's agenda was to further polarize American society, raise doubt about the integrity of the U.S. electoral process, undermine confidence in U.S. institutions, and distract the U.S. government from its responsibilities on the global stage.

Special Counsel Mueller's indictment revealed that Russian operatives from the IRA began visiting the United States in 2014 to assess our political climate. This on-the-ground penetration in 2014 and early 2015 coincided with a flurry of online activity. As ASD Non-Resident Fellow Clint Watts testified before the Senate Select Committee on Intelligence, official Russian news outlets Sputnik and RT started pushing out stories on divisive issues like the Black Lives Matter protests and tensions in the Bundy Ranch standoff in Oregon.[12] They also ran stories promoting deliberately false information and conspiracy theories, such as the bogus claim that the U.S. government would declare martial law during military exercises in Texas.[13] The Russian government established American-looking social media accounts that amplified these stories, giving them the veneer of credibility and popularity.[14] At the onset of the operation, the Russian government was preparing to undermine the 2016 election, but was more immediately focused on the broader objective of tainting democracy and democratic leaders and weakening the cohesiveness of American society.

As November 2016 approached, the IRA began to focus more specifically on the election and supporting the candidacy of Donald Trump, who Moscow assessed would enact policies more sympathetic to Russia's positions.[15] According to the Mueller indictment, part of the Kremlin's strategy involved "denigrating other [Republican] candidates, such as Ted Cruz and Marco Rubio."[16] The operation diversified in tools and tactics as Russian intelligence operatives conducted well-timed hacks of the Democratic National Committee (DNC) and Hillary Clinton's campaign chairman John Podesta and other campaign aides, hacks designed to deepen wounds between supporters of the two Democratic Party primary frontrunners, Clinton and Bernie Sanders, and to undermine Clinton's candidacy in the general election against Trump.[17] Russian intelligence services were also suspected of sharing those emails with WikiLeaks as well as setting up the website DCLeaks specifically to release hacked e-mails. Russian trolls masquerading as Americans on social media began purchasing political ads to support candidates, boost attendance at political

11 The members of the Advisory Council of the Alliance for Securing Democracy endorse this report, indicating their support for its goals, direction, and judgments. Endorsement does not necessarily denote approval of every finding and recommendation. Advisory Council members contribute to the Alliance for Securing Democracy in their individual capacities. For a list of Advisory Council members and their biographies, see Appendix B.

12 Clint Watts, "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014," *The Daily Beast*, *March 30, 2017*, https://www.thedailybeast.com/articles/2017/03/30/russia-s-info-war-on-the-u-s-started-in-2014.

13 "Jade Helm 15: Texans Terrified of Obama-Led US Army Invasion," *SputnikNews*, *July 7, 2015*, https://sputniknews.com/us/201507071024303072/; Robert Bridge, "Jade Helm 15: One Nation Under Siege?," *RT*, *July 10, 2015*, https://www.rt.com/op-ed/272920-us-army-jade-helm/.

14 Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times*, *September 7, 2017*,https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

15 "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, p. 1, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

16 U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," p. 17, February 16, 2018, https://www.justice.gov/file/1035477/download.

17 Raphael Satter, "Inside Story: How Russians Hacked the Democrats' Emails," *AP News*, *November 4, 2017*, https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a.

rallies, and inflame debate around our society's most contentious social and political issues.[18] The ads not only supported Trump and far-right positions, but as the Mueller indictment showed, they also supported Sanders and Green Party candidate Jill Stein. Accounts called "Woke Blacks" and "Blacktivist" urged Americans to vote for third-party candidates or not show up to the polls.[19]

Russian operatives also probed American electoral infrastructure by launching cyber-attacks against 21 U.S. states' voting systems and voter registration databases, targeting election officials' e-mail accounts, and breaking into a private election systems company's server and using that position as a launching point to send phishing emails to 122 state and local election officials in Florida.[20] While there is no evidence to suggest these cyber-attacks changed actual votes, the numerous cyber incursions point to vulnerabilities in U.S. electoral infrastructure and indicate Russian hackers may have been gathering information on these systems to exploit in the future. Or, these probes may have been conducted to provide a basis for raising doubts about the integrity of the electoral process if the election result had been different, to accompany Russian disinformation that the election would be rigged. There is also the question of whether the Russian government provided direct financial support to U.S. political actors and organizations, in addition to purchasing political ads and funding rallies supported by genuine U.S. political groups.[21]

What many Americans may not realize is that since the election, the Kremlin's proxies have continued their offensive. On a daily basis, they are repeatedly injecting inflammatory material into the U.S. political and social ecosystems to amplify growing social and political polarization within and between the left and right. These operations have targeted prominent Democrats as well as Republicans, including members of the Trump administration. The continued targeting of wedge issues that divide Americans, from racial equality to immigration, combined with continued cyber-attacks on U.S. critical infrastructure, is designed to destabilize American society and lay the groundwork for campaigns to undermine future elections.[22]

It is still unclear whether attempts to undermine the midterm elections in November 2018 and the presidential election in 2020 will match the scope and severity of the 2016 operation. However, Russia and other adversaries possess the capabilities and the motivation to interfere in future elections, and the overwhelming consensus among national security professionals, including members of President Trump's cabinet, is that our elections and democratic institutions are at risk of being attacked and our defenses are insufficient.

Operational and Institutional Vulnerabilities: Why the United States Failed to Stop the Threat

The Kremlin operation to undermine democracy weaponized our openness as a nation, attempting to turn our greatest strength into a weakness, and exploited several operational and institutional vulnerabilities in American government and society:

- A government that was — and remains — unprepared to address asymmetric threats of this nature;
- Insufficient cyber defenses and outdated electoral infrastructure;
- Tech companies that failed to anticipate how their platforms could be manipulated and poor cooperation between the public and private sector to address technological threats;

18 "The Social Media Ads Russia Wanted Americans To See," *Politico, November 1, 2017*, https://www.politico.com/story/2017/11/01/social-media-ads-russia-wanted-americans-to-see-244423.

19 Rachel Wolfe, "Donald Trump, Bernie Sanders, and Jill Stein All Appear to Have Been Helped By Russian Election Interference," *Vox, February 16, 2018*, https://www.vox.com/policy-and-politics/2018/2/16/17021248/russian-election-interference-sanders-stein-trump.

20 Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept, June 5, 2017*, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

21 U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Majority Staff Report: Russian Attempts to Influence U.S. Domestic Energy Markets by Exploiting Social Media, March 1, 2018*, 115th Cong. 2nd sess. https://science.house.gov/sites/republicans.science.house.gov/files/documents/3.1.18%20Publication%20Report%20Russian%20Attempts%20to%20Influence%20U.S.%20Domestic%20Energy%20Markets%20by%20Exploiting%20Social%20Media%20FINAL.pdf

22 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *United States Computer Emergency Readiness Team, Department of Homeland Security, March 15, 2018*, https://www.us-cert.gov/ncas/alerts/TA18-074A.

- A highly polarized media environment which amplified Russian disinformation without regard for the credibility of the information they reported or the ethics of doing so;
- A porous financial system that allowed dirty or anonymous money to enter the country and facilitate the aims of corrupt foreign elite;
- The polarization of American citizens and the American political system; and,
- A general decline of faith in democracy and the media.

It took significant time for the various agencies of the U.S. government to connect the dots and understand the breadth and scope of the Russian operation. Even now, more than a year and a half after the election, the full extent of Russian activities is still being uncovered. The Kremlin's interference used tools and tactics that cut across agency jurisdictions. No government agency had a full picture of the disinformation campaign unfolding on social media until after the election. Additionally, there was not a clear understanding that the Kremlin was using cyber-attacks against electoral infrastructure until approximately the summer of 2016. The cyber-attacks triggered alarm bells across the federal government — the Department of Homeland Security (DHS), the Department of State, the National Security Council, the Homeland Security Council, and the intelligence community — but some state officials overseeing their own electoral jurisdictions balked at receiving federal assistance to secure the vote and some local officials still dispute the threat environment for the 2018 elections.[23]

Politics inhibited an adequate response as well. The Obama administration was cautious in its public pronouncement regarding the unfolding attack because of concerns that the White House would be accused of trying to influence the electorate by unilaterally releasing information claiming the Russian government was conducting an operation to elect Donald Trump.[24] The administration's attempts to coordinate with Members of Congress to inform the public on a bipartisan basis were rebuffed, owing to concerns about the veracity of the intelligence and the possibility of influencing the vote in favor of Clinton.[25] Democrats and Republicans each put out their own versions of the unfolding events, further confusing the electorate. In the heat of the campaign, Donald Trump also encouraged the Russians to hack and leak e-mails of his opponent, and praised WikiLeaks for releasing the content of the e-mails.[2627]

Tech companies missed or ignored warning signs as well. None of the major social media companies had sufficient mechanisms in place to identify and shut down on a timely basis the types of falsified accounts or malicious bot accounts the Kremlin's proxies used. Twitter estimated after the fact that there were over 50,000 Russian-linked accounts during the campaign on its platform alone, while the Democratic members of the House Permanent Select Committee on Intelligence (HPSCI) revealed that there were 3,841 Twitter accounts directly connected to the IRA, some of which were opened and continued to operate after the 2016 election.[2829] The same HPSCI report noted 470 IRA-created Facebook pages with 80,000 pieces of organic content on those pages reaching more than 126 million Americans.[30] The IRA also exploited the social media companies' ethos of providing open platforms for civic and political discourse by purchasing ads in support of candidates and issues. This was a problem that traveled across platforms:

23 Philip Bump, "What Obama Did, Didn't Do And Couldn't Do in Response to Russian Interference," *Washington Post, February 21, 2018*, https://www.washingtonpost.com/news/politics/wp/2018/02/21/what-obama-did-didnt-do-and-couldnt-do-in-response-to-russian-interference/.

24 Edward-Isaac Dovere, "Biden: McConnell Stopped Obama From Calling Out Russians," *POLITICO, accessed June 5, 2018*, http://politi.co/2BpdrQi.

25 Jennifer Rubin, "McConnell Owes the Country a Fuller Explanation on Russian Meddling," *Washington Post, February 20, 2018*, https://www.washingtonpost.com/blogs/right-turn/wp/2018/02/20/mcconnell-owes-the-country-a-fuller-explanation-on-russian-meddling/.

26 Michael Crowley and Tyler Pager, "Trump Urges Russia to Hack Clinton's Email," *Politico, July 27, 2016*, https://www.politico.com/story/2016/07/trump-putin-no-relationship-226282.

27 David Choi, "5 Times Trump Praised WikiLeaks during His 2016 Election Campaign," *Business Insider, November 13, 2017*, http://www.businessinsider.com/trump-wikileaks-campaign-speeches-julian-assange-2017-11.

28 Jon Swaine, "Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed," *The Guardian, January 20, 2018*, sec. Technology, http://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed.

29 U.S. Congress, House Permanent Select Committee on Intelligence Democrats, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," June 18, 2018, https://democrats-intelligence.house.gov/social-media-content/default.aspx.

30 Ibid.

Facebook, Twitter, Instagram, YouTube, Tumblr, Reddit, 4Chan, and others were all mediums for Kremlin-linked influence operations.[31]

During the 2016 campaign, social media accounts were rife with information for journalists working for traditional media outlets as a type of *vox populi*. Unfortunately, they were rife with disinformation as well. Thirty-two of thirty-three major American news outlets used information from accounts that were later revealed to be operated by the IRA (the media continued to use IRA accounts as sources for news stories long after the election).[3233] Some of the outlets only used IRA-cited information once, but even one time is too many. In addition, media outlets eagerly reported on the information released by WikiLeaks from the DNC and Podesta hacks, often without confirming the veracity of the information or contextualizing the source of the information as obtained through illegal means by a foreign actor trying to influence the election.

Finally, the polarization of American society, reflected in our politics, exacerbated the divisions the Russian government exploited. The rise of cable news reflecting a particular political agenda, rise of social media as a primary source of news and information for many Americans, the entrenchment of echo chambers on online platforms, the spread of vitriol online, and the general debasement of civic discourse left the United States susceptible to foreign interference. These problems have not abated since the 2016 election, nor has the threat of foreign interference in American democracy. Americans must learn from all of these institutional and societal failures to address this ongoing challenge on a bipartisan basis.

II. New Technologies, Old Tactics: The Longstanding Threat to Democracies

The multifaceted operation to undermine America brought the threat of Russian malign influence operations back to the forefront of the U.S. national agenda, but the threat is not new. Deploying various tools to target foreign governments and to exploit open, democratic societies harkens back to Soviet times. During the Cold War, democracy was the Soviet Union's ideological enemy. Moscow used so-called "active measures" inside the United States and against our allies across the globe to advance the cause of communism worldwide.[34] These tactics, however, were often costly and time consuming with limited reach, in stark contrast to the ease with which technology now facilitates remote manipulation and low-cost individual targeting of any American with a smart phone and a social media account.

Post-Soviet Russia no longer has the same ideological fabric, but democracy remains the enemy of President Vladimir Putin and those who prop up his autocratic, kleptocratic regime. President Putin is concerned, above all, with maintaining his hold on power. To maintain his regime's stability and defuse the internal power struggles that threaten all autocracies, Putin ensures his control over Russia's levers of power by facilitating the enrichment of loyalists in the security services, government, and state-owned enterprises. The population sees little of the spoils of corruption – and even pays for the spoils. To justify its system of government at home, the Kremlin uses state-controlled media to push the narrative that the West is in decline and that democracy is not the superior form of government western officials would have them believe. The Russian government's operations to weaken democracies give Putin examples to highlight as he justifies his own corrupt regime to his people and maintains his grip on power.

31 Bradley Hanlon, "It's Not Just Facebook: Countering Russia's Social Media Offensive," *Alliance for Securing Democracy, German Marshall Fund of the United States, April 11, 2018*. http://securingdemocracy.gmfus.org/publications/its-not-just-facebook-countering-russias-social-media-offensive.

32 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.

33 Donie O'Sullivan, "American Media Keeps Failing for Russian Trolls," *CNNTech, June 21, 2018*, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

34 U.S. Department of State, "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," October 1981, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

According to Russian military doctrine, the NATO alliance, led by the United States, represents the primary threat to Russian national security.[35] From the Kremlin's perspective, NATO's mission to maintain peace and security in Europe and representation, along with the EU, of a community of transatlantic democratic states, runs counter to the Kremlin's interests. Putin employs a combination of low-cost tools to weaken others in order to provide Russia with greater relative power on the world stage. The Russian government's operations beyond its borders, especially campaigns waged in European countries over the past two decades, aim to fracture the cohesion of the EU and NATO, divide European allies from one another and from the United States, and weaken and distract the United States in order to assert a more aggressive posture abroad with less of a challenge from the West. Finally, the Kremlin seeks to change nations' policies towards Russia; through influence operations, it aspires to spread a more pro-Russian worldview among political, financial, civic, and media leaders in other countries that can be advantageous to Moscow's interests worldwide.

The Asymmetric Toolkit

The Kremlin employs a set of asymmetric tools to undermine democracy in other countries. Many of these tools are not new, nor are they specific to Russia, and they are often used in combination with one another to engage in political warfare.

Asymmetric tools are low-cost, often deniable measures that can counter conventional military superiority.[36] This toolkit includes:

1. Information operations: The deliberate use of false narratives through traditional and social media to mislead a population, and the amplification or weaponization of information in order to increase the polarization or undermine democratic institutions of a particular society.

2. Cyber-attacks: The penetration of computer networks to cripple critical infrastructure; disrupt the work of public and private sector actors; and, steal or alter data to inflict damage upon or cause confusion within a government, corporation, or society.

3. Malign Financial Influence: The movement of money into another country to acquire political and economic leverage and fund other asymmetric activities; and, the use of corruption as a means to recruit proxies.

4. Support for political parties and advocacy groups: The backing of politicians and groups, often at the extremes of the political spectrum, inside another country through financial, rhetorical, and other means, designed to promote a friendly agenda toward the government providing support or to support divisive or extremist views inside the host country.

5. State economic coercion: The exploitation of national resources to use as leverage over another country's government to weaken it and force a change in policy.

The use of this relatively inexpensive toolkit offsets conventional weaknesses, particularly economic limitations, and keeps adversaries off balance through their deniable and covert nature. The plausible deniability inherent in some of these measures presents challenges for democracies to respond. Often, these tools are used in the absence of kinetic military force, though in some cases, especially on Russia's periphery, they have been combined with hybrid warfare or kinetic operations, most notably in February 2014, when Russian soldiers masquerading as "little green men" in unmarked uniforms took control of Crimea, in Ukraine, and supported separatist forces in eastern Ukraine; and in August 2008, when Russian soldiers openly invaded neighboring Georgia.

This toolkit is also being used by other authoritarian governments, most notably China, to interfere in democracies. Russia's successful exploitation of democracies' vulnerabilities in Europe and the United States is likely to lead other authoritarians to adopt the Putin playbook. Concerningly, even U.S. partners are now utilizing elements of this

35 Ministry of Defense of the Russian Federation, "Voennaja doktrina Rossijskoj Federacii," December 26, 2014, http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589760.

36 Laura Rosenberger and Jamie Fly, "Shredding the Putin Playbook," *Democracy Journal, Winter 2018, No. 47*, https://democracyjournal.org/magazine/47/shredding-the-putin-playbook/.

interference toolkit. Countries including Qatar and the United Arab Emirates have reportedly used financial influence, cyber-attacks, and disinformation to attempt to influence American politics.[37]

An Overview of Russia's Asymmetric Operations in Europe

The Kremlin Russia's military interventions in Georgia in 2008 and Ukraine in 2014 were the most egregious and deadly operations to foment instability in Europe since the collapse of the Soviet Union. These interventions not only sought a geopolitical goal — to impede the Euro-Atlantic aspirations of these countries — but also directly challenged the fundamental norms and principles of the UN Charter governing the post-war liberal international order for decades, particularly the principle of states' territorial integrity and sovereignty. Along with military occupation, Moscow has used elements of the asymmetric toolkit against Ukraine: disinformation campaigns[38] spread pro-Kremlin propaganda; cyber-attacks[39] have crippled government agencies (including the Central Election Commission during the 2014 presidential elections[40]), infrastructure, private companies, and military systems; energy resources[41] (and the withholding of them) have been used as a form of coercion; and, separatists and extremists who engage in violent and destabilizing activities have been supported.

The Russian government's massive, three-week cyber-attack against neighboring Estonia in 2007 arguably gave the threat of these asymmetric tools a new sense of urgency for NATO and the EU. Since then, the three Baltic States have been hit particularly hard by Russian-originated cyber-attacks[42] and disinformation campaigns,[43] as Russia seeks to take critical infrastructure offline and sow discord between the ethnic majorities and Russian minorities of all three countries. Moscow has used both licit and illicit means to curry favor with political and economic elites in several Central and Eastern European countries, attempting to reorient their governments, economies, and societies from the EU to Moscow. We are now witnessing how many countries in Central and Eastern Europe, notably Hungary and Poland, risk democratic backsliding; while anti-democratic forces in these countries initially gained strength without external assistance, the Russian government provides various forms of financial, rhetorical, and political support to many of them.

European nations that aspire to join the EU or NATO are particular targets of Russian active measures. The Kremlin backed a failed coup attempt in Montenegro that sought to install an anti-NATO government in Podgorica.[44] A daily barrage of Russian disinformation demonizing NATO and the United States floods the media space in Serbia, while in Bosnia and Herzegovina, Moscow's support for nationalist politicians through a variety of means helps fan ethnic tensions and undercuts the country's progress toward EU and NATO accession.[45]

More recently, the countries of Western Europe, the bulwark of European values and the heavyweights of the EU, have faced destabilization operations as well. The transatlantic community, including the United States, long viewed Russian asymmetric threats as limited to the countries along Russia's periphery, such as Georgia, Ukraine,

37 Kevin Collier, "How Two Persian Gulf Nations Turned the US Media into Their Battleground," *Buzzfeed, May 9, 2018*, https://www.buzzfeed.com/kevincollier/qatar-uae-iran-trump-leaks-emails-broidy?utm_term=.eaE29g2aW#.tv5mGqmRL.

38 Ellen Nakashima, "Inside a Russian Disinformation Campaign in Ukraine in 2014," *Washington Post, December 25, 2017*, https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html.

39 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired, June 20, 2017*, https://www.wired.com/story/russian-hackers-attack-ukraine.

40 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers," *Christian Science Monitor, June 17, 2017*, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

41 Vladimir Soldatkin and Natalia Zinets, "Gazprom Seeks to Halt Ukraine Gas Contracts as Dispute Escalates," *Reuters, March 2, 2018*, https://www.reuters.com/article/us-russia-ukraine-gas/gazprom-seeks-to-halt-ukraine-gas-contracts-as-dispute-escalates-idUSKCN1GE2DW.

42 Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-based Hackers Target Baltic Energy Networks," *Reuters, May 11, 2017*, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.

43 "Baltics Battle Russia in Online Disinformation War," *DW, October 8, 2017*, http://www.dw.com/en/baltics-battle-russia-in-online-disinformation-war/a-40828834.

44 Valerie Hopkins, "Indictment Tells Murky Montenegrin Coup Tale," *POLITICO, May 23, 2017*, https://www.politico.eu/article/montenegro-nato-milo-dukanovic-murky-coup-plot/.

45 David Salvo and Stephanie De Leon, "Russia's Efforts to Destabilize Bosnia and Herzegovina," *The German Marshall Fund of the United States, April 25, 2018*, http://securingdemocracy.gmfus.org/publications/russias-efforts-destabilize-bosnia-and-herzegovina.

and the Baltic states. Few thought Moscow would extend its reach into Western Europe or across the Atlantic to North America. But such assessments were short-sighted and underestimated the threat. Putin may have perceived a lack of transatlantic resistance to Russian aggression in Georgia and Ukraine, and ultimately set his sights westward. Russian disinformation campaigns have fomented separatism and the fragmentation of Europe. In the UK, Moscow targeted the Scottish independence referendum[46] and the Brexit vote,[47] while in Spain, Kremlin-operated and other pro-Kremlin online accounts boosted support for Catalonian secession from Spain.[48] Even a Dutch referendum on the EU's Association Agreement with Ukraine became a target for Russian disinformation; the campaign against the agreement, which ultimately won the vote, used pro-Kremlin narratives pulled from RT and Sputnik and had links to Russian academics parroting Moscow's position against the agreement.[4950]

Meanwhile, in elections in France and Germany in 2017, Russian government operatives injected disinformation into the ecosystem to promote far-right groups supportive of the Kremlin's agenda, including German far-right party Alternative fur Deutschland (AfD), the first far-right party ever to clear the five-percent hurdle to enter parliament in post-war Germany.[5152] Germany also faced a Russian-led disinformation campaign, centered around false allegations that a gang of migrants raped a 13-year old German of Russian origin named Liza, that sought to increase anti-migration sentiments in the run-up to the country's parliamentary elections, arguably giving AfD a big assist in the subsequent elections.[53] Hackers likely affiliated with Russian intelligence services targeted French President Emmanuel Macron's presidential campaign's e-mail servers and leaked the contents online in the final days of the campaign.[54]

Using official news organizations like Sputnik and RT, which are amplified by Russian-linked accounts on social media, the Kremlin actively promotes alternative theories in these targeted European countries, all of them dubious and deliberately misleading, to explain away the Russian government's connection to egregious violations of international norms in Europe. Moscow has waged disinformation campaigns to argue the Russian military is not fighting in eastern Ukraine on behalf of separatist rebels and to persuade the European public that the Ukrainian military, and not the Russian-controlled separatists, downed Malaysian Airlines flight MH17, despite an international forensic investigation that unequivocally implicated the Russian military.[55] The Kremlin has also pushed false flag conspiracy theories to explain the poisoning of former British intelligence asset Sergei Skripal and his daughter Yulia in Salisbury, England, an act carried out by the

46 David Leask, "Fake Twitter Accounts Send 400,000 Independence Messages," *Herald Scotland, November 19, 2017*, http://www.heraldscotland.com/politics/referendumnews/15670523.Fake_Twitter_accounts_send_400_000_independence_messages/.

47 Robert Booth et al., "Russia Used Hundreds of Fake Accounts to Tweet About Brexit, Data Shows," *The Guardian, November 14, 2017*, sec. *World news*, http://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

48 David Salvo and Etienne Soula, "Russian Government's Fission Know-How Hard at Work in Europe," *Alliance for Securing Democracy, German Marshall Fund of the United States*, October 31, 2017, http://securingdemocracy.gmfus.org/blog/2017/10/31/russian-governments-fission-know-how-hard-work-europe.

49 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *The New York Times*, February 16, 2017, https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

50 Anne Applebaum, "The Dutch Just Showed the World How Russia Influences Western European Elections," *The Washington Post*, April 8, 2016, https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/b427602a-fcf1-11e5-886f-a037dba38301_story.html.

51 Chloe Farand, "French Social Media is Being Flooded With Fake News, Ahead of the Election," *The Independent*, April 22, 2017, http://www.independent.co.uk/news/world/europe/french-voters-deluge-fake-news-stories-facebook-twitter-russian-influence-days-before-election-a7696506.html; Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," *Brookings Institution, June 28, 2017*, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

52 Anne Appelbaum, Peter Pomerantsev et al., "'Make Germany Great Again:' Kremlin, Alt-Right and International Influences in the 2017 German Elections," *Institute for Strategic Dialogue, December 6, 2017*, https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf.

53 Michael Weiss, "The Kremlin Cries Rape for Propaganda in Germany," *The Daily Beast, February 2, 2016*, https://www.thedailybeast.com/the-kremlin-cries-rape-for-propaganda-in-germany.

54 Alex Hern, "Macron Hackers Linked to Russian-Affiliated Group Behind US Attack," *The Guardian, May 8, 2017*, sec. *World news*, http://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

55 Mike Corder, "Netherlands, Australia Hold Russia Liable for Downing MH17," *The Associated Press, May 25, 2018*, https://apnews.com/4b05cd0e43c84e74822eb1356337ccdf; "Defensive Disinformation as Decoy Flare: Skripal and Flight MH17," *EU vs Disinfo, March 27, 2018*, https://euvsdisinfo.eu/defensive-disinformation-as-decoy-flare-skripal-and-flight-mh17/.

Russian intelligence services, and to claim that the West deliberately staged chemical weapons attacks against Syrian civilians as a pretext to launch missile strikes against Bashar al-Assad's regime.[56] These information operations have a singular purpose: by promoting falsehoods frequently and loudly enough, the Kremlin perpetuates a public discourse that denigrates the value of facts, making it more difficult for Europeans to maintain a united front in the face of Russian aggression on the continent and beyond.

The Russian government has even expanded its activities to regions of the world in which it seeks to regain some of the influence the Soviet Union once enjoyed. In Latin America, for example, senior officials in the Trump administration have warned there is mounting evidence that the Kremlin is again employing its disinformation army to influence public opinion and potentially elections in Mexico.[57]

III. A New Strategic Approach for Government and Society

As the Kremlin achieved success with its tools and tactics in the United States and across the transatlantic community, democratic governments and societies' vulnerabilities to asymmetric operations have been exposed for others to exploit. In a world increasingly interconnected by technology, state and non-state actors alike will be able to conduct malign influence operations of varying scales and sophistication. As other foreign actors enter the field, Western institutions, such as the EU and NATO, and democracies worldwide will face additional challenges. China has moved beyond its economic-driven approach to gain influence in other countries and has started adopting more overt forms of political interference in countries like Australia and New Zealand, as well as in Taiwan and Hong Kong.[58] Autocrats like Philippines President Rodrigo Duterte and Turkish President Recep Tayyip Erdogan are using these tools against their own citizens, with Duterte building his own "keyboard army" to silence dissent and Turkish pro-government trolls hacking, harassing, and threatening journalists.[59][60]

Technology will continue to advance faster than governments and society can adapt. Today's disinformation operations will look amateur compared to what is coming in the future. Tools that allow for precise doctoring of audio, images, and video will make it even more complicated to discern fact from fiction. Algorithms, which already drive much of the operations of major social media platforms, will hold increasing sway as artificial intelligence plays a larger role in the technology that powers our daily lives. Cyber tools may allow foreign actors to penetrate more deeply into government and corporate networks to steal information, disrupt elections, and compromise individual privacy without much of a trace. The challenges we face today will grow by an order of magnitude. That is why all parts of democratic societies must be involved in exposing influence operations, as one of the best methods to preventing future attacks is to shine sunlight on existing ones, and in shaping our responses. The threat to democracies' stability is clear. But our focus now needs to be on not just understanding the problem, but defending against and deterring it going forward.

Whole of Government

Much like the 9/11 attacks demonstrated how government had to reorient itself to confront a potent, unconventional, asymmetric threat in global terrorism, defending against foreign interference operations demands a new strategic approach. The failure to unearth and respond to the operation against the 2016 election in a timely manner revealed how necessary it is for government to detect these threats in an integrated manner, involving all relevant players in the interagency, and to respond to them holistically

56 DFRLab, "#TrollTracker: Disinformation Surge from Skripal to Syria," *Medium, April 17, 2018*, https://medium.com/dfrlab/trolltracker-disinformation-surge-from-skripal-to-syria-f44f92a476cd.

57 "Tillerson Warns Mexico to Watch Russian Election Meddling," *Reuters, February 2, 2018*, https://www.reuters.com/article/us-mexico-usa-russia/tillerson-warns-mexico-to-watch-russian-election-meddling-idUSKBN1FM2MO.

58 Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response | The Asan Forum," May 8, 2018. http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/.

59 "Freedom of the Net 2017," *Freedom House, November 14, 2017*, https://freedomhouse.org/report/freedom-net/2017/philippines.

60 Maeve Shearlaw, "Turkish Journalists Face Abuse and Threats Online Trolls Step Up Attacks," *The Guardian, November 1, 2016*, https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-threats-online-trolls-attacks.

and strategically, rather than in silos. The Executive Branch and Congress must therefore rectify existing bureaucratic and structural impediments to improve coordination between federal agencies and between the federal, state, and local governments. In particular, the cross-cutting nature of the threat demands the allocation of sufficient resources to address it and the harnessing of expertise across the policy and intelligence communities under one roof. The national security community should also develop greater expertise on asymmetric and emerging threats.

But bureaucratic fixes are only part of the solution. An effective, long-term strategy must start by putting the issue at the forefront of the U.S. national security agenda, with the public recognition that foreign actors' attempts to weaken the United States and our allies by undermining democratic institutions constitute a threat to national security. That will require clear strategic messaging from the top. A decisive signal from the administration at the highest level and from Congress that the United States considers these activities a threat to national security and will respond accordingly is essential for making clear to adversaries and allies alike that the U.S. government takes the threat seriously. A united front by the President, the Cabinet, and leading Members of Congress can help facilitate better coordination between the federal government and state and local governments to bolster defenses at all levels. Strong leadership from Washington can also raise awareness and build resilience in society toward a threat that affects the average American just as it affects the political establishment in Washington. Through effective public messaging, the White House and Congress can also help transcend the politicization of civic discourse that malign foreign influence operations exploit to further divide Americans from one another. It is essential that America's enemies as well as U.S. partners that may be tempted to utilize similar tools in their quest for influence realize that there will be repercussions for violating U.S. laws and undermining American democracy.

Distrust between the Executive Branch and Congress hindered the U.S. government's ability to respond to the Russian operation against the 2016 election. Partisan distrust has prevented Democrats and Republicans, as well as the White House and Congress, from taking urgent action to defend our nation. This distrust and politicization of a national security threat have impeded necessary work by the Trump administration and Congress to fully secure electoral infrastructure, prevent foreign money from influencing public opinion during political campaigns, develop effective means to work with the technology community to address technological vulnerabilities, and close legislative and regulatory loopholes that allow foreign actors to use money to peddle political influence. America's leaders are essentially leaving the country undefended against a threat that is only growing

Removing partisanship from the calculus in responding to this threat is critical to ensuring our elected representatives and government officials take actions to secure our democracy. Legislation that establishes clear indicators of foreign interference in elections and other democratic institutions and processes and mandates that the Executive Branch report to Congress when those tripwires are crossed would correct two deficiencies from 2016: first, it would allow an incumbent administration to report information to Congress and the public without being accused of trying to affect the results of an election; and second, it conceivably would create conditions for Members of Congress to reach across the aisle and act in the public interest.

Foreign operations to destabilize our democracy will continue to be a threat long into the future. And foreign adversaries will continue to take advantage of a polarized, hyper-partisan political climate, so long as it exists. It is short-sighted — and indeed, emboldens adversaries like Vladimir Putin — when politics gets in the way and political leaders fail to take action to protect the institutions that make America what it is.

Raising the Cost on Our Adversaries

Raising the cost of conducting these operations against the United States must be another essential pillar of government's strategic approach to addressing this threat. Government should resist the temptation of responding tit-for-tat to every active measure. There will be times when a symmetric response is necessary, including proportionate cyber responses

to cyber-attacks and potentially offensive cyber-attacks as a deterrent. But government generally needs to breakdown the individual silos through which it addresses each tool in the asymmetric toolkit. Instead, the administration and Congress should define and use our own asymmetric advantages and strategically deploy instruments of national power that will serve as the most effective deterrent. This approach will allow democracies to play to their advantage, rather than responding on an adversary's terms, and provide the best chance of inducing a foreign actor to change behavior.

In the case of Russia, the Putin regime places regime survival above all other objectives and is dependent on the corrupt financial links that tie together the political leadership, security services, and business. To impose real consequences on the Kremlin that could lead to behavioral change, U.S. policy should play to our own strengths and focus on exploiting Russia's comparative economic weaknesses by using sanctions, asset forfeiture, and anti-money laundering tools to target the illicit wealth of individuals and entities that assist the Kremlin's destabilizing foreign policy actions, and by exposing the ill-gotten gains of top Russian officials, including President Putin himself. Such an approach should hit politically important elements of the elite hardest, increasing political pressure and heightening internal dissent. Tracking and disrupting financial stocks, flows, and new investments will make it more difficult for the Kremlin to fund malign influence activities abroad and gain access to sensitive technology or data. Even transparency about legitimate Russian investments in democratic countries is important to limit the danger that Russian economic influence will inappropriately impact politicians and their decision-making in other countries. Such measures will also serve to strengthen our own democracies, rooting out pathways for corruption. To the greatest extent possible, these measures should be multilateral, taken together with our European allies and partners, as well as democratic allies and partners around the world. A transatlantic focus on illicit finance will deny those who benefit from kleptocracy the ability to enjoy its fruits in the West.

Imposing reputational costs on authoritarian powers that employ these tools must also be part of the counter-arsenal. Vladimir Putin values his standing on the world stage. That is why it is so important that Russia not be allowed to reenter normal international fora until Russian behavior changes. Just as Europeans should halt their recent renewed engagement of Russia in the wake of President Trump's withdrawal from the JCPOA, the Trump administration should not encourage Russia's re-admission to gatherings of the world's major economic and democratic powers. Authoritarians need to know that democratic interference brings with it a cost that will not fade with the passage of time. This is as true for China as it is for Russia. The Chinese Communist Party is more sensitive about being exposed for illegal activity and interference operations abroad, as China attempts to sell an alternative model of governance and growth to developing nations.[61] Imposing reputational costs on Beijing must be a pillar of western deterrence strategy.

Governments cannot reasonably expect to stop every type of asymmetric operation. Cyber-attacks will continue, as will attempts to mislead public opinion through disinformation campaigns. The challenge of responding to asymmetric threats like foreign interference operations is that the attackers attempt to exploit a gray zone — neither outright warfare that affects hard security assets, nor soft power that seeks to influence a foreign public through benign measures like commerce or educational exchanges. The reality, however, is that these tactics are a direct attack on democracy and should be treated as such.

That said, the U.S. government must resist emulating the tactics used by authoritarian regimes when responding to these threats. We have learned from our history that when we seek to carry out covert subterfuge to undermine democratic processes abroad, including elections, it frequently backfires, undermining our credibility and our values on the global stage.

Moreover, the measures we take to respond to malign foreign influence operations must not themselves undermine democracy. That includes ensuring the protection of free speech and privacy rights while addressing the manipulation of our information ecosystem. We should remain committed to promoting democracy abroad and supporting global actors who are working to make their governments more responsible and societies more open. U.S. foreign

61 Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," *Open Forum, The ASAN Forum*, May 8, 2018. http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response.

assistance is not – and never will be – equivalent to the covert, subversive operations run by the Kremlin and other authoritarian regimes. The U.S. government supports measures to strengthen democracy through transparent governance, anti-corruption, free and fair elections, and empowered citizen participation in all aspects of democratic society. These are the ideals we should continue to support beyond our borders, and we should be proud to defend them from false comparisons to the tools and tactics authoritarian regimes use overseas. And above all, we should be working actively to improve our own democracy at home, which will not only strengthen us as a nation but will also make our institutions and society more resilient to this threat.

The American people deserve a government that has positioned itself to do the best possible job. Treating the problem as an urgent matter of national security, putting aside partisan strife, maximizing efficiency, strategically formulating policy responses, and adhering to the values that make democracy the prevailing global ideal will enable the U.S. government to address this challenge adequately and responsibly.

A Transatlantic Threat Demands a Transatlantic Response

The United States and its European allies make up an integrated, transatlantic community. For decades, this integration through NATO and the U.S.-EU relationship has provided all member states security, material benefit, and leadership in the world. Defending against threats to our democracies therefore requires an integrated, coordinated response. Democracies will rise and fall together. Cracks in democratic institutions in one country contribute to an overall weakening of the liberal democratic order. The United States must maintain its leadership role at NATO and its strong partnership with the EU in order to strengthen the Alliance's capabilities to address asymmetric threats and work in concert with Brussels to deter malign foreign influence operations.

Both the EU and NATO have begun to address how they defend against asymmetric challenges like Russian influence operations. NATO has established Centers of Excellence that analyze components of the hybrid toolkit, while a handful of EU member states support another Center of Excellence in Helsinki, Finland that looks at the problem more holistically. Meanwhile, in Brussels, the EU's East StratCom Task Force counters Russian disinformation campaigns directly, while in April, the European Commission released a comprehensive report with policy recommendations to combat disinformation spread online.[62]

These efforts are a good start, and both organizations have made the hybrid challenge a priority. Like the United States, European nations, along with the EU, will have to do more to build resilience to cyber-attacks, combat money laundering and other forms of illicit finance from Russia and other foreign actors that ends up in the pockets of politicians and other influential Europeans. The EU should also guard more firmly against democratic backsliding within member states, which plays into the hands of authoritarian regimes, while also increasing support for independent media, civil society, and other democratic actors in the Western Balkans and Eastern Partnership states.

We must learn lessons from each other to determine the most effective defense and deterrence measures and the most successful responses. This means better bilateral cooperation between the EU and the United States on issues like data privacy and protection, cyber hygiene, policies that address disinformation threats on social media, and transparency with the public on asymmetric threats. It also means NATO and EU member states must show a greater willingness to exchange information on new tactics that Russia and other foreign actors are deploying against us, in multi-nation formats, rather than just bilaterally between governments. The G7's recent commitment to share information and work with social media companies and internet service providers to prevent foreign interference in elections could be an impetus for more efficient transatlantic coordination to share threat information and best practices.[63] Finally, the EU and NATO, individual governments, and non-governmental organizations should combine their respective strengths and expertise and form

62 European Commission, "Communication – Tackling Online Disinformation: A European Approach," April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

63 "Charlevoix Commitment on Defending Democracy from Foreign Threats," *G7 2018 Charlevoix*, June 10, 2018. https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats.

a coalition to address malign foreign influence operations across the full asymmetric toolkit. A coalition that meets regularly and provides virtual opportunities to share open source information and analysis, and to coordinate responses in real time will enhance our collective ability to secure democracies.

The threat that foreign interference poses to democracies is not limited to the transatlantic community. Democracies around the world – from Latin America to Australia and New Zealand – are increasingly facing challenges from authoritarian governments like China and Russia. The United States and European governments should work with all of their allies and partners to defend democracies, and a public-private coalition to address malign foreign influence operations should ultimately compromise officials and experts from democratic countries worldwide, possibly utilizing existing fora, such as the Community of Democracies, where democracies gather to discuss shared challenges.

Whole of Society Approach

While the government's role is essential, the nature of these threats requires that the private sector and civil society be involved in the solution. The private sector, particularly tech companies, will have a critical role in addressing technological vulnerabilities and building resilience against malign foreign influence operations. The potential of social media companies to transform the way people around the globe interact with one another and how they access information and serve as a democratizing force is important. However, as with any new creation, these platforms have significant vulnerabilities as well as benefits – and our adversaries identified those vulnerabilities before the companies or U.S. government did, weaponizing and turning the platforms against their users in ways the companies never envisioned.

Tech companies thus far have responded slowly and without the full transparency the American people deserve to determine how Russian government operatives exploited their platforms. Much of the companies' response has seemed more focused on damage control than on transparency and a willingness to tackle the fundamental issues at hand. Self-regulation alone to try and tackle the weaponization of social media ultimately will be insufficient. Congress should take narrowly scoped, smart steps, such as the proposed Secure Elections Act or introducing legislation to have bots identified and labeled as such, to ensure that foreign actors do not use social media platforms to interfere in U.S. elections, and protect Americans' personal information online.[64] However, government should avoid overreach, and legislation will never be able to keep pace with technological change. As technologies become more sophisticated over time, the challenge to the tech sector will be even greater. The companies will need to be much more proactive in addressing threats of abuse and misinformation on their platforms and more transparent with their users to detect and deter such activities in a timely manner.

As technology continues to evolve, tech companies should develop processes, including through engagement with outside researchers, national security experts, and civil society, to maximize the upsides of new tools and platforms and minimize the downsides before they are used more broadly, or our adversaries will continue to exploit them before we become aware of vulnerabilities. This should include developing a more constructive partnership with government and outside researchers to share information on influence operations that target their platforms. This is particularly important as malign actors seamlessly move across platforms in order to drive influence campaigns. Meaningful public-private partnerships will help overcome the trust gap that exists between Washington and the tech community and foster consensus on solutions to existing and future vulnerabilities foreign actors exploit.

Social media companies do not operate in a vacuum. In particular, their business models depend on other corporations that buy advertisements. Private companies can play their own part in demanding that tech companies address malign foreign influence operations more thoroughly by using their ad buys as leverage to force change from companies on these issues and threatening to pull their ads from platforms that do not take necessary steps, as several companies have already done. Not only would these corporations put pressure on the

64 United States Congress, Senate, *Secure Elections Act*, S 2261, 115th Cong., 1st sess., https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

tech sector by diminishing the economic value of extreme and highly viral, malign content, but they would help raise awareness among society about the extent of the threat we are facing.

More broadly, American businesses are custodians of democracy, just as government and individual citizens are. Their prosperity has been built on it and benefits from it. The business community can take on a larger role as custodians of democracy by reinforcing the importance of democratic institutions among the American public, investing in civil society organizations that address the problem of foreign interference, and supporting other pillars of democratic society, like free and independent journalism. Businesses have a stake in protecting our democracy; after all, their prosperity will be directly threatened by the weakening of our institutions.

Addressing the societal vulnerabilities that the Russian government exploited is also a challenge for civil society. In the aftermath of the 2016 election, think tanks in Washington, NGOs, and researchers across the country rose to that challenge and began playing an instrumental role in monitoring and exposing disinformation campaigns and other forms of malign foreign influence in the United States, Canada, and Europe. Many of these organizations are playing a leading role in formulating policy and legislative solutions for the U.S. government and Congress, as this report seeks to accomplish.

Civil society can also step in and fulfill functions that government performs less effectively. For example, the State Department's Global Engagement Center (GEC), despite its dedicated staff, budget, and mandate, should not be the primary U.S. messenger for countering disinformation abroad. Foreign citizens already suspicious of or hostile to the U.S. government will be more open to indigenous actors. Therefore, the GEC should fund local civic organizations overseas that expose and raise awareness about foreign influence operations and counter the narratives the Kremlin and other foreign actors spread through traditional and social media. Along with USAID, it should also support independent media and local journalism in countries that are particularly susceptible to foreign disinformation and anti-U.S. narratives.

In the United States, civil society should play a prominent role in raising awareness about such threats and exposing and countering falsehoods propagated by foreign actors, while the government should fund watchdog groups conducting these activities. Across the United States, organizations are also working on building stronger curriculum for public education on the civic virtues of democracy, on developing media literacy programs to help children and adults understand how to discern disinformation in traditional and social media, and on recommending journalistic standards for reporting on weaponized information and using social media accounts as sources. Congress and state governments should support their efforts as well.

An Urgent Call to Action to Secure Democracy

The number of foreign actors waging malign influence campaigns against the United States and its allies and partners is growing. Absent a concerted pushback by government and the other pillars of democratic society, authoritarian regimes will continue to refine their asymmetric playbook and the use of these new technologies to run more sophisticated, insidious, and far-reaching operations against democracies, making this a core national security challenge.

The adage that a strong national security starts at home has never been more true. Defending against and deterring the use of this toolkit demands urgent bipartisan action. The recommendations in this report represent common sense measures that government and lawmakers — regardless of party affiliation — and other parts of society can take. They are endorsed by the Advisory Council of the Alliance for Securing Democracy, a bipartisan and transatlantic group of former senior national security officials, and were developed in consultation with numerous experts, government officials, and civil society representatives in the United States and Europe.

IV. Recommendations for the U.S. Government

1. Articulate publicly a declaratory policy on foreign interference in democratic institutions and processes. We recommend the President issue the following statement:

> "Malign foreign interference operations designed to destabilize the elections, institutions, and societies of the United States and its allies through asymmetric means constitute a national security threat. There will be consequences for nation states that conduct these covert, corrupting, and coercive operations. The U.S. government will respond utilizing all appropriate tools."

2. Raise the cost of conducting malign influence operations against the United States and its allies. Imposing a broader set of sanctions, cyber responses, and reputational costs against individuals and organizations that support malign foreign influence operations, facilitate corruption, and prop up authoritarian regimes conducting foreign interference would not only impose costs on adversaries, but would potentially serve as a deterrent against future operations.

The Administration should:

- Employ cyber responses as appropriate to respond to cyber-attacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats.

- Expand sanctions against wealthy Russian individuals and strategic industries that assist Putin's destabilizing foreign policy actions, as called for by congressional legislation. The Countering America's Adversaries Through Sanctions Act (CAATSA) calls for sanctions against a broader list of individuals and entities tied to Russia's intelligence and defense sectors. The administration, which signed CAATSA into law, should adopt a similarly tougher stance. In particular, the Department of Treasury's Office of Foreign Assets Control has the authority to target foreign persons for providing material support to already-sanctioned actors, as well as targeting foreign persons operating in Russia's energy, defense, financial, or mining sectors. Treasury's Financial Crimes Enforcement Network has the authority to target foreign financial institutions "of primary money laundering concern" operating anywhere in the world. Both of these authorities should be used to target foreign banks that help facilitate illicit Russian financial activity, whether it stems from public corruption, organized crime, or state-backed political interference.

- Impose sanctions against a wider range of individuals and entities not only inside Russia, but also inside Iran, China, and North Korea, who use ill-gotten gains to fund malign influence operations abroad.

Congress should:

- Conduct rigorous oversight of the administration's implementation of CAATSA. To date, the administration has failed to adhere to all aspects of the legislation and Congress is failing in its duty to hold the administration responsible for implementing legislation.

- Pass legislation, such as the bipartisan DETER Act, which would trigger sanctions on Russia if the Director of National Intelligence determines the Kremlin interferes in a future U.S. election, and would prohibit the purchase of Russian sovereign debt and any state-connected bonds by U.S. citizens and entities, plugging a significant loophole Russia could use to evade sanctions.

3. Separate politics from efforts to unmask and respond to operations against the U.S. electoral process. An incumbent government must be able to respond to an attack on our electoral system without being susceptible to accusations of political machinations. Political parties and campaigns should also commit to not disseminate weaponized information illegally obtained by foreign actors.

- Congress should institute mandatory reporting requirements so that an administration must inform lawmakers of attacks against U.S. electoral infrastructure, including individual political campaigns. Reporting requirements should have a low threshold, so

administrations can present data to Congress and, if unclassified, to the public, without being accused of politicizing information to swing an election.

- The Democratic and Republican Parties and their candidates, along with other parties and independent candidates running for office, should pledge jointly not to weaponize hacked information during election campaigns. Without such a public, bipartisan promise, foreign state actors and cybercriminals could be emboldened to continue the activity they conducted during the 2016 presidential campaign.

- Parties, candidates, and outside political groups should also pledge to fully uphold existing legal restrictions that outlaw foreign contributions to the U.S. political system.

4) Improve election security and protect other critical infrastructure from cyber-attacks immediately. It is possible to secure our electoral infrastructure without infringing upon states' control of our elections. The federal government must make additional resources and assistance available to states to ensure that Americans know their most fundamental right is protected.

The Administration should:

- Maintain the designation of electoral systems as critical infrastructure.

- Through the U.S. Election Assistance Commission (EAC) and in coordination with the Department of Homeland Security (DHS), assist state and local election officials with conducting post-election audits of election results that provide a high level of confidence in the accuracy of vote totals, adopting cybersecurity standards for electoral infrastructure, and upgrading outdated infrastructure.

- Through the FBI and in consultation with DHS, inform state and local governments, political parties and campaigns, and companies that provide election-related infrastructure, when they have been hacked and help them respond. DHS should also ensure information is declassified quickly and appropriately to share with political parties and campaign staff, and others who may have a need to know but do not possess security clearances. The Belfer Center's Election Cyber Incident Communications Coordination Guide provides an excellent blueprint for DHS' Election Infrastructure Government Coordinating Council to manage communication on cyber-attacks with all relevant stakeholders in the electoral process.[65]

- Through the Office of the Director of National Intelligence (ODNI) and in coordination with DHS, the intelligence community should notify Congress, states, and relevant local election officials immediately of potential cyber breaches of their electoral infrastructure.

- Just as the Transportation Security Administration conducts random checks of airport screening systems, DHS should create a mechanism for simulating red team cyber-attacks on state and local electoral infrastructure. These simulations should feed into a policy process involving federal, state, and local officials that identifies and closes cyber vulnerabilities and improves responses to cyber-attacks.

- Through DHS, build a national classified cyber information-sharing network that appropriately cleared personnel of private companies maintaining the nation's critical infrastructure can access, in accordance with the steps outlined in a Council on Foreign Relations report.[66]

Congress should:

- Adopt legislation, such as the Secure Elections Act, to improve information sharing throughout government on election cybersecurity threats;

65 "Election Cyber Incident Communications Coordination Guide," *Belfer Center for Science and International Affairs, Harvard University, February 2018*, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsGuide.pdf.

66 Robert K. Knake, "Sharing Classified Cyber Threat Information With the Private Sector," *Council on Foreign Relations, May 15, 2018*, https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector.

provide technical resources for election agencies; and improve information sharing between the federal, state, and local levels.[67]

- Enact requirements for the federal government to notify states and relevant local election officials of intrusions into electoral infrastructure, and for the Executive Branch to notify Congress — both in a timely manner. Legislation should also require private vendors and operators of electoral infrastructure to report cybersecurity incidents that could impact the integrity of voting systems and databases to the FBI and DHS.
- Require DHS to issue security clearances to senior state government officials in charge of securing electoral infrastructure in order to facilitate access to information on threats.
- Codify into law the designation of electoral systems as critical infrastructure.
- Prioritize federal funding for cybersecurity research and development.
- Pass legislation to elevate the DHS National Protection and Programs Directorate into a full-fledged operational agency under DHS jurisdiction; one bill has already been introduced and is being considered by Congress.[68] The agency should facilitate improved coordination across government on responses to cyber threats to all 16 critical infrastructure sectors.

State and local governments should:

- Accept federal assistance on election security. While it is not a federal government competency to run elections, states lack the resources and expertise that the federal government possesses on cyber threats to critical infrastructure.
- Comply with EAC's voluntary voting system guidelines and the National Institute of Standards and Technology's cybersecurity framework for critical infrastructure.
- Make mandatory the use of electronic voting machines that issue a voter verified paper ballot, and the conduction of post-election audits of paper voting records to corroborate electronic results.
- Conduct an audit and threat analysis of voter registration systems, and upgrade systems as necessary, as recommended in a Brennan Center for Justice report.[69]

5) Appoint a Foreign Interference Coordinator at the National Security Council and establish a National Hybrid Threat Center at the Office of the Director of National Intelligence. The Coordinator and Threat Center would direct policy formulation and intelligence analysis respectively on the range of asymmetric tools and interference operations designed to destabilize the United States and its allies. A policy decision should be made to elevate foreign interference on the list of intelligence collection and analytical priorities, with responsibility for intelligence coordination residing in the Hybrid Threat Center. The President, Congress, and the American people should have confidence in the intelligence community's sources of information that corroborate an interference operation and an adversary's intent to undermine U.S. democracy.

NSC Foreign Interference Coordinator

- We recommend the President appoint a Foreign Interference Coordinator at the National Security Council (NSC) because the NSC is responsible for coordinating among the many individual agencies that handle a subset of these issues (DOD, State, Treasury, DHS, and others).

67 United States Congress, Senate, Secure *Elections Act*, S 2261, 115th Cong., 1st sess., https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

68 United States Congress, House, *Cybersecurity and Infrastructure Security Agency Act of 2017*, HR 3359, 115th Cong., 1st. sess., https://www.congress.gov/bill/115th-congress/house-bill/3359/text.

69 Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," *Brennan Center for Justice, New York University School of Law*, June 29, 2017, https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf.

- The Coordinator should have sufficient staff from the interagency and be given the authority to coordinate across the NSC and to task agencies on policy and intelligence collection priorities on foreign interference. The Coordinator would be the primary U.S. government official in charge of presenting policy options to the President to address malign foreign influence operations, and for coordinating with allies and partners on these issues.

- To give the Coordinator significant standing in the interagency, the President should appoint a former senior U.S. official — ideally a former Cabinet-level official or former Member of Congress — to the position. This official should ideally be a Deputy Assistant to the President and report directly to the National Security Adviser and through him or her to the President.

- The Coordinator would be responsible for working with Congress to ensure the proper laws, regulations, and authorities are in place to deter and respond to asymmetric attacks.

- The Coordinator and his/her staff should establish strong ties with the private sector — tech companies, financial institutions, and corporations that manage critical infrastructure — and civil society organizations to cultivate an effective working relationship with non-government actors to address various types of asymmetric threats.

Hybrid Threat Center at the Office of the Director of National Intelligence (ODNI)

- The Hybrid Threat Center at ODNI should bring together experts from across the intelligence community who are tracking individual elements of the asymmetric toolkit. Policymakers need to be informed of how foreign adversaries use the various tools in tandem; the Threat Center would ensure experts on cyber, finance, economics, disinformation, leadership, and regional affairs are working in unison to assess influence operations holistically.

- The Hybrid Threat Center should also track influence operations domestically and overseas against the United States and its allies. When possible, it should make information available to the public regarding trends, threats, and tactics deployed by authoritarian adversaries. It would supplant existing task forces at individual agencies, whose mandates and resources are limited by their particular mission and budget. For example, the FBI's foreign influence task force is bound by the FBI's criminal and counterintelligence mandates within the United States. Combining these functions into a center that also has responsibility for overseas collection would give the intelligence community and policymakers greater visibility into nebulous, cross-border operations. The intelligence community and Congress should work together to resolve the existing legal limitations on parts of the intelligence community to monitor disinformation operations. The intelligence community and Congress should ensure the appropriate legal authorities are in place to protect the privacy and civil liberties of U.S. citizens. The very fact that it is often difficult to distinguish the sources and origins of operations and individual accounts necessitates strict congressional oversight and appropriate authorities to ensure intelligence agencies have the information necessary to protect the homeland while protecting American's privacy rights. Lessons learned from post-9/11 counterterrorism experiences should be applied to the foreign interference threat. Congress should legislate reporting requirements for the Threat Center to report on its activities and implications for privacy and civil liberties.

- The Hybrid Threat Center should allocate significant resources to monitoring open source information, particularly on social media, to analyze disinformation campaigns and the weaponization of information and ensure that open source intelligence is given the appropriate weight in analytic products.

- The Hybrid Threat Center should also monitor technological trends, particularly important in cyber and disinformation, so policymakers can adapt the government's responses accordingly.

6. Close loopholes that allow foreign actors to unduly influence our political system. Foreign actors exploit existing laws and regulations to move money into the United States that can ultimately affect the American political system. There are several measures the administration and Congress can take to update regulations and pass legislative solutions to close off illicit finance and covert political influence from abroad.

The Administration should:

- Track flows of international funds transfers to, from, or through the United States by creating a centralized database at the Department of Treasury of all international funds transfers that transit the country. Large U.S. banks that clear dollars for international payments would report the data on a near real-time basis. The reporting streams could then be combined, providing a complete view of U.S. dollar transactional activity. The idea has been studied by Treasury but never finalized, although Canada and Australia collect similar information. While international funds transfer records are available on an ad hoc basis, only a centralized database would drive the type of powerful analysis that is necessary. Over time, payments data could be married up with securities trade data collected under a new system called the Consolidated Audit Trail that is currently being put in place by the Securities and Exchange Commission; shipping data collected by Customs and Border Patrol; and other information sources that would facilitate illicit finance network analysis.

- Require title insurance companies to report to Treasury the beneficial owners of legal entities used to purchase any residential or commercial property nationwide. This would provide a defense against foreign buyers who purchase a house, condo, or commercial property in the United States without forming a U.S. company or opening a U.S. bank account. A temporary Treasury order now requires purchasers of high-end residential real estate in select cities to report identifying information and has detected a great deal of suspicious activity, but the order is neither comprehensive nor permanent.

- Use existing civil and criminal penalties to punish financial institutions and their employees involved in illicit financial activity, including for violations of sanctions or violations of money laundering statutes. Money laundered into the United States is also potentially subject to criminal or civil asset forfeiture.

Congress should:

- Pass legislation, such as Honest Ads Act, to improve disclosure requirements for online political advertisements so that Americans understand who is funding political ads they see online. Furthermore, as recommend in a report[70] by the Brennan Center for Justice, Congress should also: Ensure through legislation that the source information explaining the origins of online political ads remains attached to posts when those ads are shared on social media; and mandate that social media companies selling political ads use the credit card industry's address verification system to determine whether an ad buyer has a U.S. billing address.

- Pass legislation to have bots identified and labeled.

- Reform the Foreign Agents Registration Act (FARA) so all agents of foreign governments are appropriately registered in the United

70 Ian Vandewalker and Lawrence Norden, "Getting Foreign Funds Out of America's Elections," *Brennan Center for Justice, April 6, 2018*, https://www.brennancenter.org/publication/getting-foreign-funds-out-americas-elections.

States. There are a number of bills introduced by Members of Congress on both sides of theaisle that Congress should consider. [71]

- Establish a beneficial ownership regime for company formation. Passing a law requiring beneficial ownership reporting at the time of company formation, such as this recent House bill, is essential.[72] Importantly, it enjoys the support of the financial services industry.[73]

- Expand the jurisdiction of the Committee on Foreign Investment in the United States' (CFIUS) and provide it additional resources. CFIUS, an interagency body responsible for reviewing inbound foreign investment for national security risks, should be permitted to review a broader range of transactions, particularly in critical technology, artificial intelligence, and the media sector, and from countries that pose national security risks, such as Russia and China.

7. Increase assistance to allies and partners to ensure they have the ability to withstand and respondtoattemptstounderminetheirdemocratic institutions. Due to historical and cultural ties and resource dependencies, some European nations are particularly vulnerable to Russian asymmetric campaigns. Others are complicit in facilitating illicit financial flows. U.S. allies and partners in Asia are also increasingly vulnerable to Chinese influence operations. The United States must utilize various forms of assistance to strengthen allies and partners' democratic institutions, governments, and societies. The U.S. government should also institutionalize more regular coordination with European allies and partners to address the threat of foreign interference, and should work with democracies in Asia to better understand the threats they face from Chinese interference, help them withstand that challenge, and learn lessons from other countries' experiences.

- The administration should utilize effectively the increase in U.S. foreign assistance to European and Eurasian states that Congress has mandated, particularly through CAATSA. This assistance should be used to build democratic resilience throughout the region and increase societal resistance to the Kremlin's tactics, such as its support for political and social groups and its use of disinformation to exacerbate existing social divisions.

- Congress and the administration should ensure that they appropriate and use sufficient resources to strengthen democratic institutions and civil society in allied and partner countries in order to combat Russian, Chinese, and other forms of malign foreign influence operations.

- The administration should help our European allies and partners reduce energy dependence on Russia by continuing to press key European governments to oppose the Nord Stream 2 pipeline project.

- The administration and Congress should reduce European energy dependence on Russia by updating the regulations that allow U.S. companies to export liquefied natural gas (LNG) to Europe to make the process faster and more flexible while maintaining environmental safeguards.

- The Department of Treasury should establish a program to provide technical assistance to countries, like Latvia, seeking to strengthen their ability to combat illicit finance.

71 United States Congress, House, *Disclosing Foreign Influence Act*, HR 4170, 115th Cong., 2nd. sess., introduced in House October 31, 2017, https://www.congress.gov/bill/115th-congress/house-bill/4170/text; United States Congress, House, *Foreign Entities Reform Act of 2018*, HR 5331, 115th Cong., 2nd. sess., introduced in House March 19, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5331/text; United States Congress, House, *Foreign Influence Transparency Act*, HR 5336, 115th Cong., 2nd. sess., introduced in House March 20, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5336/text; United States Congress, Senate, *Disclosing Foreign Influence Act*, S 2039, 115th Cong., 1st. sess., introduced in Senate October 31, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/2039/text; United States Congress, Senate, *Foreign Agent Lobbying Transparency Enforcement Act*, S 1679, 115th Cong., 1st. sess., introduced in Senate July 31, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1679/text; United States Congress, Senate, *Foreign Agents Registration Amendments Act of 2018*, S 2482, 115th Cong., 2nd. sess., introduced in Senate March 1, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2482/text; United States Congress, Senate, *Foreign Agents Registration Modernization and Enforcement Act*, S 625, 115th Cong., 1st. sess., introduced in Senate March 14, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/625/text; United States Congress, Senate, *Foreign Influence Transparency Act*, S 2583, 115th Cong., 2nd. sess., introduced in Senate March 21, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2583/text;

72 United States Congress, House, *Counter Terrorism and Illicit Finance Act*, HR 6068, 115th Cong., 2nd. sess., introduced in House June 12, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6068/text.

73 The Clearing House Association et al., "To Representatives Pearce and Luetkemeyer," January 4, 2018, https://www.sifma.org/wp-content/uploads/2018/02/Counter-Terrorism-and-Illicit-Finance-Act.pdf.

- The Departments of State and Treasury should increase diplomatic efforts to convince countries of key concern in facilitating illicit finance, such as Cyprus, to implement critical reforms. Incentives could include additional U.S. foreign investment, extended technical assistance, and support for the re-establishment of direct correspondent banking ties.

- The U.S. government should work with European allies and partners to establish a transatlantic coalition on defending democracies.

- The United States should increase efforts with partners, including Europe, Taiwan, Japan, Australia, South Korea, and India to provide alternatives to China's Belt and Road Initiative.

8. Contribute to efforts to building societal resilience to foreign interference in the United States and abroad. Government should help raise awareness about the threat of foreign interference, as exposure is one of the most effective means to combat foreign interference operations. However, it should also seek partners who can combat foreign disinformation and effectively message to American and foreign audiences, and who are devoted to strengthening democratic values worldwide. This is as important domestically as it is overseas. Thirty years ago in his farewell address to the nation, President Reagan expressed concern about "an erosion of the American spirit" and called on Americans to focus more attention on "American history and a greater emphasis on civic ritual."[74] This challenge is even greater today.

- Congress and the Executive Branch should endorse the work of civil society and private sector groups promoting civics education and media literacy programs in the United States and authorize the Department of Education to work with state governments that establish statewide civics and media literacy programs.

- The Department of State's Global Engagement Center and Office of the Coordinator of U.S. Assistance to Europe and Eurasia, together with USAID, should support civil society organizations in Europe that track and counter foreign disinformation. Similar partnerships should be developed to more effectively track growing Chinese influence operations.

- DHS or the White House, through the proposed NSC Foreign Interference Coordinator, should implement a Public Service Announcement (PSA) campaign that promotes smart cyber behavior and raises awareness about various types of foreign interference affecting U.S. citizens, businesses, and institutions. The federal government has had PSA campaigns on a myriad of issues, from quitting smoking to stopping pollution. Threats of foreign interference that affect all Americans should receive similar treatment.

9. Ensure that data privacy laws protect U.S. ctizens' personal information on social media platforms. It is increasingly apparent that the United States needs a legal framework for protecting U.S. citizens' data, given repeated breaches, privacy concerns, and acquisition by foreign adversarial governments. Lawmakers and tech companies will have to find a balance between European-style regulation that potentially stifles innovation and a regulatory framework that protects data privacy and allows free enterprise to thrive.

V. Recommendations for the European Union and NATO

1. Establish an International Coalition on Defending Democracies. European governments, together with the United States, Canada, EU, NATO, and Five Eye allies Australia and New Zealand, should establish a forum for sharing information and analysis, exchanging best practices, and coordinating policy and programmatic responses to defend democracies from malign foreign influence operations. Coordination between governments is currently taking place on an ad hoc basis, and tends to be stovepiped by each element of the toolkit — cyber experts conduct exchanges, as do experts on disinformation and strategic communication. What the transatlantic community needs is regular contact between governments assessing the entirety of the asymmetric toolkit holistically, so governments and international organizations can prepare more effective responses. There

74 Ronald Reagan, "Farewell Address to the Nation," *The American Presidency Project, January 11, 1989*, http://www.presidency.ucsb.edu/ws/?pid=29650.

should also be a formalized Track II channel for non-government representatives and organizations to enter into a dialogue with government officials on policy solutions. Such a channel could be particularly important for the public and private sectors to exchange best practices and lessons learned on data privacy and cyber issues with a view towards developing norms that could be adopted by governments. The coalition should eventually incorporate governments and experts from democracies worldwide, as transatlantic countries can learn much about the experiences of democracies in Asia, Latin America, and elsewhere.

2. Strengthen the sanctions regime to match measures taken by the U.S. government. The Kremlin is counting on European fatigue toward the existing sanctions regime. The best way to demonstrate that the EU takes Russian government efforts to destabilize the transatlantic community seriously is for member states to agree on additional sanctions on Russian individuals and entities that complement the recent sanctions imposed by the U.S. government. The EU should also extend the six-month review period for sanctions to 12 months, reducing the opportunities for member states to break consensus in Brussels. It is essential that the Trump administration and European governments do not remove sanctions or reduce diplomatic pressure on the Putin regime until Russia ceases its malign activities in Ukraine and the rest of Europe as well as the United States. Imposing other reputational costs, such as halting rapprochement with Russia or implementing the European Commission's recent recommendation for member states to improve their capabilities to publicly attribute cyber-attacks, should also be part of Europe's strategy to increase deterrence and raise costs on adversaries.[75]

3. Institute a Joint NATO-EU Task Force on Countering Asymmetric Threats. At the 2016 Warsaw Summit, NATO and the EU agreed to enhance their cooperation on hybrid and cyber threats, relying on their respective military and non-military strengths and capabilities to complement each other's efforts. The upcoming NATO summit in Brussels in July 2018 will likely produce more concrete actions on hybrid threats for the Alliance, while the European Commission, drawing partly on the work of the High Level Expert Group on Fake News and Online Disinformation, has issued recommendations on combatting disinformation online.[76] These are welcome steps. However, at the moment, each organization has disparate elements that monitor aspects of the Russian toolkit, but are not all well-funded or in synch with one another's efforts. A Joint Task Force could better coordinate these various efforts, and would also serve as an important mechanism to keep the United Kingdom integrated in European efforts to strengthen common defenses against asymmetric threats post-Brexit. It should perform the following functions:

- Conduct joint analysis of threats, both at the working level and at the North Atlantic Council, as well as exchanges of technical expertise between the relevant bodies within the EU and NATO, including cyber threats to EU and NATO member state networks. This would require a mechanism for sharing classified information, which currently does not exist between the two organizations. On threats of this magnitude, there should be a medium for NATO Allies and EU partners to exchange threat information.

- Coordinate the various lines of effort on hybrid threats, particularly on disinformation and cybersecurity, conducted by the Centers of Excellence at NATO, the East StratCom Task Force at the EU, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, the High Level Experts Group on Fake News and Online Disinformation, and other parts of the EU bureaucracy.

75 "Joint Communication to the European Parliament, the European Council and the Council: Increasing Resilience And Bolstering Capabilities to Address Hybrid Threats," *European Commission, June 13, 2018*, https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

76 "Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling Online Disinformation: A European Approach," *European Commission, April 26, 2018*, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

- Monitor disinformation campaigns on social media and in traditional media that seek to undermine the organizations or destabilize a member state, and coordinate responses, as appropriate.

- Develop norms of behavior for cyberspace that would guide NATO and EU member states' own actions, as well as their responses to cyber threats. This could serve as a model for global cyber norms.

- Deploy personnel at the request of member states for assistance in defending against, deterring, or responding to a malign foreign influence operation.

- Bolster public outreach by communicating to the European public within member states and within aspirant countries. NATO and the EU can jointly advocate for the benefits of the transatlantic community and why it represents a superior alternative to the geopolitical orientation and form of government proposed by authoritarian regimes like Russia.

4. Shut down channels for money laundering and other forms of illicit finance. The Russian government exploits lax regulations and corrupt banking practices to move money into Europe and peddle political influence. Just like the United States, Europe too needs to close these loopholes.

- Establish an EU central body to combat money laundering. This central body should have the authority to examine banks, impose fines, revoke licenses, and/or restrict operations of financial institutions without needing to wait for national authorities of a member state to submit a recommendation.

- The European Central Bank (ECB) should apply its existing authorities — including prudential supervision, approval of purchases of "qualified holdings" in banks, and fit and proper review — to illicit finance matters when there is reason to believe that there may be ongoing anti-money laundering violations.

- The EU should explore how to better utilize euro payments data, either via TARGET2 (the leading European platform for processing large-value payments, used by central banks and commercial banks to process euro payments in real time) or at the national level, to detect illicit financial activity and use such information as the basis for targeted reviews or referrals to regulators and law enforcement agencies.

- EU member states should continue to enhance information sharing to combat illicit financial activity, as it is planning to do under the Fifth Anti-Money Laundering Directive. By more robustly sharing transactional data, supervisory information, law enforcement information, and classified intelligence across borders, member states will achieve better results in detecting and disrupting the activity of illicit financial facilitators who operate across member states' borders.

- The European Commission should review current passporting arrangements[77] and consider whether adjustments would be appropriate to prevent the evasion of appropriate supervisory oversight.

5. Support the pillars of democratic society within EU member states and in the surrounding neighborhood. An important way to prevent democratic backsliding in Europe – and buttress resilience to authoritarian regimes' attempts to destabilize the transatlantic community – is to strengthen civil society and free and independent media. The EU should:

- Maintain pressure on EU member states to uphold European democratic values, such as allowing a free and independent press to flourish, keeping the judiciary independent from political influence, and supporting civil society.

77 According to Investopedia, "Passporting is the exercise of the right for a firm registered in the European Economic Area (EEA) to do business in any other EEA state without needing further authorization in each country."

- Increase funding for NGOs that monitor and expose disinformation campaigns and corruption, particularly in vulnerable regions like the Western Balkans.

- Support programs that strengthen free and independent media, particularly in countries that aspire to join the EU but are susceptible to Russian disinformation and destabilization operations (e.g., Serbia, Bosnia and Herzegovina, Kosovo, Montenegro, Ukraine, and Georgia). Pro-Kremlin narratives easily spread through local media outlets through Russian state-sponsored news agencies RT and Sputnik. Only by supporting homegrown journalism can local media outlets report objectively on a broad range of issues without having to rely on Russian propaganda for content.

VI. Recommendations for the Private Sector

1. Be more transparent about their technology, business models, and how platforms can be manipulated. The tech sector has reluctantly and belatedly released information to Congress and the public about the manipulation of social media platforms to undermine democracy, but there are several steps tech companies should take to be more transparent:

- Design platforms so that they provide explanations for users about how and why content appears for them, and make those explanations easy to understand for the public. The companies should also explain what they are doing to refine algorithms and counter efforts to exploit them.

- Make more accessible company policies that determine how user data is collected, and make privacy controls easier for users so they can consent or prevent their information from being collected, including by malevolent foreign actors.

- Facilitate third-party research into disinformation campaigns on and across social media platforms. Most social media platforms make it difficult for researchers to analyze data trends, because their application programming interfaces (APIs) are closed to the general public. While tech companies are engaging in a broader discussion about their policies and technologies in a limited way, they need to remove the blindfold and allow researchers to look at the data, ensure accountability in the tech sector, and recommend cross-platform solutions to prevent the distortion of information online.

- The tech companies should ensure they first involve legal and data protection experts, who can make clear to the public what should and should not be shared with outside experts.

2. Create mechanisms for collaboration on defending against disinformation and cyber-attacks. Many disinformation campaigns and cyber threats do not just manipulate one platform; the information moves across various platforms or a cyber-attack threatens multiple companies' network security and data integrity. There must be greater cooperation within the tech sector and between the tech sector and other stakeholders to address these issues.

- As recommended in a NYU Stern Center report, tech companies should conduct across-the-board internal assessments of disinformation threats. [78] The tech companies are too large for any one individual or department to have the answers. Bringing together engineers, business leads, customer support, legal, trust and safety teams, and policy experts from across the company should lead to changes that protect users and weed out harmful content.

- Policy changes within individual companies are a meaningful start, but sufficiently addressing these cross-platform threats will require multiple stakeholders. Therefore, all relevant tech companies should participate in a collaborative forum for sharing analysis and solutions to combat disinformation and cyber-attacks. Models for cooperation already exist

78 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights, New York University*, November 3, 2017, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform-companies-fighting-terrorist-incitement-and-politically.

and can be developed further: Google, Facebook, Twitter, and Microsoft already maintain a common database of digital fingerprints identifying violent extremist videos.[79] These four companies also participate in a Cyberhate Problem-Solving Lab run by the Anti-Defamation League's Center for Technology and Society.[80] Dozens of tech companies participate in the Global Network Initiative, a tech policy forum devoted to protecting digital rights globally.

3. Build a more constructive public-private partnership, particularly to identify emerging technological threats. It is imperative that the tech sector and government develop a more constructive partnership. New technologies, such as "deep fake" audio and video doctoring, will make the next wave of disinformation even harder to detect and deter.

- The tech sector and national security professionals should work together to identify potential vulnerabilities in new and existing technologies that can be exploited by adversaries, and strengthen defenses and deterrence measures. The two sectors should also establish a mechanism to share data to identify nefarious actors on social media platforms linked to foreign nation states, while ensuring protection of Americans' privacy and free speech.

- The data exchanged between the government and tech sector should also be briefed to Congress and made available to the public to maximize transparency.

- There needs to be more funding for research of new technologies and their potential misuse for disinformation. The Pentagon's Defense Advanced Research Projects Agency (DARPA)'s own research on identifying deep fakes, combined with grants it has awarded outside researchers, is a positive development.[81]

- As recommended by Brookings Institution experts, the public and private sectors need to be working together to assess the responsible design and use of decentralized applications, which utilize blockchain technology and other peer-to-peer tools.[82]

4. Enact clear guidelines for verifying users and content and taking down accounts and content that violate Terms of Service (TOS). While some European governments have taken steps to regulate content on social media, the protection of free speech, enshrined in the First Amendment, is paramount in the United States. Companies bear a heavy responsibility to ensure that their platforms are not abused or used as tools to spread the type of disinformation intended to undermine either individual rights or democratic institutions. While European-style regulation may not be the answer in the United States, the companies must take action on harmful content consistent with their TOS. For example, some of Facebook and Twitter's new requirements for political ad purchasers to verify their identity are a good step, though have faced challenges in implementation.[83] The platforms face real difficulties in managing an enormous volume of organic content and an environment where malicious users and accounts linked to nation-state malign influence operations or authoritarian regimes thrive. These bad actors can flood the system with illegitimate TOS complaints, hoping the content or accounts they disapprove of will simply be pulled without deliberation. A combination of human and algorithmic review must be in place to monitor content and accounts. Social media companies should take the following steps:

- Devote more human resources to auditing complaints regarding TOS violations and develop clearer, more rigorous guidelines for removing content while protecting free speech.

79 "Partnership to Help Curb Spread of Online Terrorist Content," *Facebook Newsroom, December 5, 2016*, https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content.

80 "Facebook, Google, Microsoft, Twitter, and ADL Announce Lab to Engineer New Solutions to Stop Cyberhate," *Anti-Defamation League*, October 10, 2017, https://www.adl.org/news/press-releases/facebook-google-microsoft-twitter-and-adl-announce-lab-to-engineer-new.

81 Taylor Hatmaker, "DARPA Is Funding New Tech That Can Identify Manipulated Videos and 'Deepfakes,'" *Tech Crunch, April 30, 2018*, https://techcrunch.com/2018/04/30/deepfakes-fake-videos-darpa-sri-international-media-forensics.

82 Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy, May 25, 2018*, http://foreignpolicy.com/2018/05/25/disinformation-wars.

83 Mark Glaser, "Facebook's Political Ad Disclosures Are a Train Wreck in Progress," *Digital Context Next, June 7, 2018*, https://digitalcontentnext.org/blog/2018/06/07/facebooks-political-ad-disclosures-a-train-wreck.

- To the best of their ability, more clearly articulate to users the reasons why they removed users' content or blocked their account, and allow for users to appeal the decision.[84]

- Consider ways to amplify verified content and marginalize suspicious content.

- Continue to refine AI tools that can spot bot accounts that are manipulating social media platforms. Many bot accounts are benign or beneficial, such as those that issue Amber Alerts and other public service announcements. Legislation that mandates that bots be identified and labeled will help provide transparency, as will adding additional human resources to managing this challenge. However, the sheer volume of bot accounts makes the use of AI essential. The foreign interference challenge cannot be successfully addressed solely through the hiring of additional personnel.

- Platforms must also permit authenticated accounts operated by human beings to remain publicly anonymous. Maintaining anonymity is important not only for users who wish to have a greater degree of privacy, but also for activists and political opposition figures in authoritarian states.

5. Examine the implications of the business model that underpins these companies. The ad-driven, engagement-focused revenue stream adopted by the major social media companies has also created a medium for malicious actors, like the Internet Research Agency in St. Petersburg, to exploit. Although platforms like Facebook and YouTube have taken some steps to address this, with Facebook requiring disclosures of political ads and YouTube promising to improve algorithms to keep advertisers' ads away from harmful content and vowing to remove more offensive videos, a broader discussion on disentangling advertising from data collection is worth having.[85] Less individualized, more contextual advertising like we see on other media — TV and print, for example — may make it more difficult for nefarious actors to target specific segments of the population with harmful content (violent extremists and terrorists) or falsified content for political purposes (nation-state actors). A report by New America's Public Interest Technology program offers some guiding principles for thinking through this challenge.[86]

6. Invest more in civil society's efforts to combat foreign influence operations. American businesses are custodians of democracy, just as government and individual citizens are. Their prosperity has been built on it and benefits from it, and they should play a role in protecting it from foreign interference.

Corporations that have philanthropic arms, as well as private foundations, should be more involved in defending against foreign actors' attempts to destabilize democracies. Investing in organizations that run media literacy campaigns, expose disinformation and corruption, and conduct free and independent journalism, particularly on the local level, should be a priority for corporations and philanthropists.

84 Erica Newland et al., "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," *The Berkman Center for Internet & Society and The Center for Democracy & Technology, September 2011*, https://www.cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf.

85 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights, New York University, p. 27, November 3, 2017*, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform-companies-fighting-terrorist-incitement-and-politically.

86 Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," *New America, January 23, 2018*, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit.

VII. Recommendations for Media Organizations[87]

1. Confirm the veracity of leaked information and be judicious about using it. Hacking operations by states and non-state actors are now a feature of political life in the democratic world. But the actors behind the hacks have an agenda, and that agenda can be enabled if media are not careful about how they report the story. The illegally-obtained information that nefarious actors steal and WikiLeaks and others publish can only be weaponized successfully if journalists publicize the contents of the hacks. Even after the 2016 experience with the DNC and John Podesta's hacked emails, reporters continue to traffic in material hacked by foreign actors, as recently shown in the Qatari-Emirati influence feud.[88] To report responsibly on weaponized information, journalists should:

- Distinguish between reporting on hacking operations and reporting on the content of the leaked information. During the 2017 presidential campaign in France, French journalists covered the story of the hack of then-candidate Emmanuel Macron's campaign e-mails and the online data dump. However, to prevent amplifying potentially falsified information and to avoid being a part of politicizing the operation, they refrained from reporting on the content of the data. Contrast that approach to U.S. media's reporting on the hacking and data dump of DNC and Clinton campaign e-mail accounts, which injected a foreign state's political agenda into an already hyper-politicized environment.

- Verify any information before it is published and contextualize in reporting both how it was obtained and the motivations behind the hack.

2. Create guidelines for using social media accounts as sources in stories. Looking ahead to future elections, media organizations can implement the following guidelines for using social media sources:

- Use two-step verification of social media accounts before publishing information. First, ensure that the social media platform has verified the account. And second, establish contact with the user on the phone. Written contact via direct message or e-mail is insufficient to establish the authenticity of a user account. Unverified social media accounts should require additional investigation to identify the account user.

- Cite verified social media posts more responsibly by quoting them rather than embedding them. Furthermore, when embedding a tweet, consider cutting out the part that shows replies, retweets, and favorites. This avoids providing a potentially inaccurate snapshot of an account's popularity or legitimization of the information due to the account's alleged popularity. For example, the IRA frequently used bots to make these accounts appear more popular than they otherwise would have been. Media organizations used information from falsified accounts operated by the Russian government and embedded their tweets in the articles, showing readers that the accounts had a popularity, reach, and significance they did not deserve.[89][90]

3. Build story literacy, particularly for complex, rapidly developing pieces of news. Throughout journalistic history, there have always been stories with many players, parts, and subtexts. But considering today's 24/7 media environment, the overwhelming volume of information an audience can consume, and the fact that many people do not follow a story from start to finish, reporters need to go to greater lengths to synthesize material.

87 The recommendations in this section are largely derived from the following report:

Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," *Alliance for Securing Democracy, German Marshall Fund of the United States*, March 23, 2018, http://securingdemocracy.gmfus.org/publications/responsible-reporting-age-irresponsible-information. Heidi Tworek is a non-resident fellow at the German Marshall Fund of the United States.

88 United States District Court, Central District of California, Western Division, "Broidy Capital Management LLC, Elliott Broidy, and Robin Rosenzweig v. State of Qatar, Stonington Strategies LLC, Nicolas D. Muzin, and Does 1-10," March 26, 2018, https://www.documentcloud.org/documents/4451449-Broidysuit.html.

89 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.

90 Donie O'Sullivan, "American Media Keeps Falling for Russian Trolls," *CNNTech*, June 21, 2018, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

Summarizing and repeating information as stories evolve can help an audience digest them. Some tools we suggest are:

- Using timelines and network diagrams to map out key players and events in multilayered stories.
- Create a dedicated vertical to a theme that encompasses many high-profile and breaking articles, such as Russian interference in democracies. This would put all relevant stories in one location for users to find information.
- Break down complicated stories by using Q&As and explainer cards.

4. Increase transparency in reporting practice and reporting procedure. In an era of heightened suspicion towards the press, greater transparency can help the public better understand how journalism works and why journalists report what they do. Media organizations could consider taking the following steps:

- Participate in The Trust Project, a new initiative that is developing transparency standards for news consumers to assess the quality and credibility of journalism. Journalists would explain why they wrote a particular story, sources they used, previous versions of the story, etc.
- Require freelancers to disclose their sources of funding and any possible conflicts of interest. This will help prevent manipulation of freelancers and could weed out fake freelancers.
- Write stories about journalistic procedure. In other words, explain to the public how journalists do their jobs. Entire TV series have been devoted to shedding light on a profession. Public interest stories on a reporter's approach to a particular story or source could generate interest in the news outlet while simultaneously increasing transparency.

5. Anticipate future problems in journalism today. Today's disinformation campaign may not look like tomorrow's threat. The technology that is used by millions of people around the world – and exploited by a handful of state and non-state actors – will continue to evolve rapidly. Leaked and weaponized information will change over time. Campaigns did not have to worry about their e-mails being dumped onto WikiLeaks over a decade ago. Now they do. Media organizations need to stay on top of emerging trends, tools, and threats to get ahead of future challenges rather than having to issue corrections that undermine their credibility after the fact.

- Assign responsibility for disinformation and emerging threats to a C-level executive within the news organization. The executive would be in charge of finding solutions to verify potentially falsified information.
- Create a regular schedule for revisiting and updating social media verification guidelines.
- Follow BuzzFeed's lead and assign a beat reporter to cover disinformation trends and technologies to keep its audience updated on the latest developments.

VIII. Recommendations for Civil Society

1. Extend the dialogue about foreign interference in democracies beyond Washington. In several European countries, governments and non-governmental organizations are leading outreach about Russian active measures beyond their capitals in order to build societal resilience. For example, the Swedish government distributed pamphlets to 4.7 million households explaining how to prepare for war or other national crises, including cyber-attacks on national infrastructure.[91] Estonia and other governments' intelligence agencies publish annual threat assessments for public consumption. The U.S. government can conduct similar PSA campaigns, but in the United States, non-governmental organizations will be better positioned than government to fulfill different types of resilience building functions. Civil society therefore needs to be more active outside the Beltway in raising awareness, depoliticizing the debate about addressing this threat, and getting buy-in for solutions.

91 "Sweden Sends Out Leaflets on How To Prepare for War," *BBC News*, May 22, 2018, https://www.bbc.com/news/world-europe-44208921.

- Think tanks traditionally provide analysis and recommendations to decision-makers in the government. They should also advocate and act. Domestic outreach programs that bring policy experts in the think tank community in contact with their fellow Americans can be mutually beneficial. Outreach across the United States can accomplish the following: Steer this conversation away from its politicized roots in the 2016 elections and toward the broader threat that malign foreign influence operations pose to our democratic institutions; Educate fellow citizens on the seriousness and urgency of solving the problem and on the ways their lives are affected by it; Identify trusted voices among local publics, officials, businesses, and civic leaders to participate in crafting solutions on the federal, state, and local levels.

- Non-governmental organizations should advance media literacy across the country to give Americans the tools they need to distinguish fact from fiction. Several European countries — Sweden, The Netherlands, Germany, and the Czech Republic, among others — have robust media literacy programs run by NGOs and, in Sweden's case, government agencies. These programs train educators, parents, and students in best practices for critical consumption of media, and develop materials for school curricula. There are American NGOs like the News Literacy Project already dedicated to working on media literacy. Other organizations, like many of Washington's think tanks, have networks throughout the country and in Europe to leverage, including in countries that have had success in promoting media literacy. NGOs should partner together to: Conduct trainings for the public, particularly for students, about disinformation campaigns and how to avoid being manipulated when consuming news.; Advocate to state and local governments to include media literacy in their public education curriculum; Devise curriculum to strengthen civic education, particularly on the question of why democracy matters and why it should be protected from external attempts to undermine it.

2. Expand efforts to monitor and counter disinformation campaigns. Projects like ASD's Hamilton 68 Dashboard, the Atlantic Council's DFR Lab, and StopFake have been groundbreaking in exposing disinformation campaigns across the transatlantic space in real time. They should continue to refine their tools and their analytical models, and they should also be more involved in directly countering falsehoods propagated by foreign actors and perpetuated by bots and trolls online. There also needs to be more of these sites and tools, and better coordination between them to avoid duplication of efforts and to amplify each other's successes. The Atlantic Council's Disinformation Portal, with which ASD partners, is a good initial step in this direction.

- NGOs need greater funding to keep up with this rapidly developing space. Government's primary role in the disinformation field should be to issue grants to support NGOs' work. Philanthropic and private foundations should also increase their support for civil society organizations monitoring and defending against foreign threats to democratic institutions.

3. Increase support for local and independent media. Today's media environment is dominated by the cable news networks, and, to a lesser extent, the major papers. Local and independent media are dying. That is bad for a number of reasons, including the fact that local media are often trusted to a greater degree than cable and online news outlets.[92]

- Philanthropic support is essential to supporting local journalism. In addition to direct support for news outlets, individuals and foundations should support initiatives like the Report for America project, which seeks to support a new generation of emerging journalists reporting on under-covered topics in under-covered communities. With more resources, local media can indeed be a bulwark against foreign interference and disinformation.

92 Knight Foundation, "American Views: Trust, Media and Democracy," *A Gallup/Knight Foundation Survey, January 16, 2018*, https://kf-site-production.s3.amazonaws.com/publications/pdfs/000/000/242/original/KnightFoundation_AmericansViews_Client_Report_010917_Final_Updated.pdf.

4. Pressure elected officials to take this threat seriously and address it immediately. Americans across the country have the power to make their voices heard and demand that government in Washington and in their states take action to defend against and deter foreign interference in our democracy. Concerned citizens should band together to form advocacy groups in order to raise awareness and put pressure on their elected representatives.

5. Remember that our democracy is only as strong as we make it. The polarization of American society, reflected in our politics, contributed to the conditions that the Russian government exploited. Americans have a responsibility to strengthen our democracy and address our problems at home that malign foreign actors use against us. We recommend that civil society organizations form partnerships with each other and, where appropriate, with the U.S. government to improve governance and the rule of law, fight corruption, and promote media literacy. Moreover, we need to instill a healthier respect for one another, regardless of our differences, by improving our civic discourse, practicing more responsible behavior on social media, and calling on our elected officials to take action to defend our democracy on a bipartisan basis.

Acknowledgements

The authors would like to thank President of the German Marshall Fund (GMF) Karen Donfried, GMF Executive Vice President Derek Chollet, and the GMF Board of Trustees for their support for the Alliance for Securing Democracy (ASD) and dedication to strengthening the transatlantic relationship.

We would like to thank the members of ASD's Advisory Council, who provided extensive feedback on the analysis and recommendations of this report and who so generously have devoted their time and expertise to our overall mission since ASD was founded in July 2017. We also thank ASD's principal donors – the Hewlett Foundation, Democracy Fund, Sandler Family Foundation, Seth Klarman, and Craig Newmark Philanthropies – and dozens of individual donors for their support and generosity.

We are indebted to the innumerable experts whom we consulted for input, drawing on their experience in government, the tech sector, media, and civil society. We also acknowledge the vast contributions to the literature these experts have made, and on whose reports and commentary we have relied; we list several of these influential reports in Appendix A.

European officials and colleagues in various nongovernmental organizations have been gracious with sharing lessons learned from their nations' experiences confronting Russian and other foreign interference in their democracies, even when Americans should have listened to their warnings and advice well before the United States found itself under attack.

We could not have completed this report in a timely manner without the help and dedication of ASD's staff and many interns, who assisted us in all aspects of this endeavor.

Finally, we thank Americans across our country and across multiple sectors and organizations who have begun to organize and collaborate to tackle this urgent challenge to our democracy.

Appendix A: Influential Publications

The authors would like to acknowledge the substantial contribution of the following publications to the development of this report and to the furthering of research in the field of countering authoritarian influence in democracies:

Anne Appelbaum, Peter Pomerantsev et al., "'Make Germany Great Again:' Kremlin, Alt-Right and International Influences in the 2017 German Elections," *Institute for Strategic Dialogue*, December 6, 2017.

Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation," *Atlantic Council*, March 5, 2018.

"Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017.

Belinda Li, "The Other Immigration Crisis," *Hudson Institute*, January 17, 2017.

Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018.

Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," *New America*, January 23, 2018.

Edward Lucas and Peter Pomeranzev, "Winning the Information War: Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe," *Center for European Policy Analysis*, August 2016.

Erica Newland et al. "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," *The Berkman Center for Internet & Society and The Center for Democracy & Technology*, September 2011.

European Commission, "Communication - Tackling Online Disinformation: A European Approach," April 26, 2018.

"Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights*, November 3, 2017.

Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, October 13, 2016.

Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," *Alliance for Securing Democracy, German Marshall Fund of the United States*, March 23, 2018.

Ian Vandewalker and Lawrence Norden, "Getting Foreign Funds Out of America's Elections," *Brennan Center for Justice*, April 6, 2018.

"Joint Communication to the European Parliament, the European Council and the Council: Increasing Resilience And Bolstering Capabilities to Address Hybrid Threats," *European Commission*, June 13, 2018.

Jonas Parello-Plesner, "The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond," *Hudson Institute*, June 20, 2018.

Keir Giles, "Countering Russian Information Operations in the Age of Social Media," *Council on Foreign Relations*, November 21, 2017.

Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," *Brennan Center for Justice*, June 29, 2017.

"Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" (United States Senate, Committee on Foreign Relations, January 10, 2018).

Robby Mook, Matt Rhoades, and Eric Rosenbach, "Cybersecurity Campaign Playbook," *Belfer Center for Science and International Affairs*, November 2017.

Robby Mook, Matt Rhoades, and Eric Rosenbach, "The State and Local Election Cybersecurity Playbook," *Belfer Center for Science and International Affairs*, February 2018.

Robert D. Blackwill and Philip H. Gordon, "Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge," *Council on Foreign Relations*, January 2018.

Robert K. Knake, "Sharing Classified Cyber Threat Information With the Private Sector," *Council on Foreign Relations*, May 15, 2018.

Tim Maurer and Erik Brattberg, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," *Carnegie Endowment for International Peace*, May 23, 2018.

U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," February 16, 2018.

U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018.

Appendix B: ASD Advisory Council

Mike Chertoff

Mike Chertoff was U.S. Secretary of Homeland Security from 2005 to 2009. There, he worked to strengthen U.S. borders, provide intelligence analysis, and protect infrastructure. He increased the Department's focus on preparedness ahead of disasters, and implemented enhanced security at airports and borders. Following Hurricane Katrina, Chertoff helped to transform FEMA (Federal Emergency Management Agency) into an effective organization. He also served as a judge on the U.S. Court of Appeals Judge from 2003–05. He co-founded the Chertoff Group, a risk-management and security consulting company, and works as senior of counsel at the Washington, DC law firm Covington & Burling.

Toomas Ilves

Toomas Hendrik Ilves was elected president of the Republic of Estonia in 2006 and in 2011. During his presidency, Ilves was appointed to serve in several high positions in the field of information and communication technology in the European Union. He previously served as minister of foreign affairs and as the ambassador of the Republic of Estonia to the United States and Canada in Washington. Ilves was also a member of the Estonian Parliament, as well as a member of the European Parliament, where he was vice president of the Foreign Affairs Committee. He now co-chairs the World Economic Forum working group The Global Futures Council on Blockchain Technology and is a distinguished visiting fellow at the Hoover Institution at Stanford University.

David Kramer

David J. Kramer joined Florida International University's Steven J. Green School of International and Public Affairs as a senior fellow in the Vaclav Havel Program for Human Rights and Diplomacy in May 2017. Before moving to Miami, Kramer had worked in Washington, DC for 24 years, most recently as senior director for Human Rights and Democracy with The McCain Institute for International Leadership. Before that, he served for four years as president of Freedom House. Prior to that, he was a senior transatlantic fellow at The German Marshall Fund of the United States. Kramer served eight years in the U.S. Department of State during the George W. Bush administration, including as assistant secretary of state for Democracy, Human Rights, and Labor; deputy assistant secretary of state for European and Eurasian Affairs; professional staff member in the Secretary's Office of Policy Planning; and senior advisor to the undersecretary for Global Affairs. Kramer is a member of the board of directors of the Halifax International Security Forum and a member of the advisory council for the George W. Bush Presidential Center's Human Freedom Project.

Bill Kristol

William Kristol is the editor at large of the influential political journal, *The Weekly Standard*. Before starting that magazine in 1995, Kristol served in government, first as chief of staff to Secretary of Education William Bennett during the Reagan administration, and then as chief of staff to Vice President Dan Quayle in the George H. W. Bush administration. Kristol has also served on the board of the Project for the New American Century (1997–2005) and the Foreign Policy Initiative (2009–17). Before coming to Washington in 1985, Kristol taught government at the University of Pennsylvania and Harvard University.

Rick Ledgett

Rick Ledgett has four decades of experience in intelligence, cybersecurity, and cyber operations, including 29 years with the National Security Agency where he served as deputy director from January 2014 until his retirement in April 2017. In that capacity he was responsible for providing foreign intelligence and protecting the nation's most important national security-related networks. Rick is a senior visiting fellow at The MITRE Corporation, a director on the Board of M&T Bank, serves as a trustee on the Board of the Institute for Defense Analyses, and is a member of several corporate advisory boards.

Michael Morell

Michael Morell was acting director of the Central Intelligence Agency in 2011 and again from 2012 to 2013, and had previously served as deputy director and director for Intelligence at the Agency. In his over thirty years at the CIA, Morell played a central role in the United States' fight against terrorism, its initiatives to halt the proliferation of weapons of mass destruction, and its efforts to respond to trends that are altering the international landscape — including the Arab Spring, the rise of China, and the cyber threat. He was one of the leaders in the search for Osama bin Laden and participated in the deliberations that led to the raid that killed bin Laden in May 2011. He has been with Beacon Global Strategies as a senior counselor since November 2013.

Mike McFaul

Michael McFaul served for five years in the Obama administration, first as special assistant to the president and senior director for Russian and Eurasian Affairs at the National Security Council at the White House from 2009 to 2012, and then as U.S. ambassador to the Russian Federation from 2012–14. He is currently professor of political science, director, and senior fellow at the Freeman Spogli Institute for International Studies, and the Peter and Helen Bing senior fellow at the Hoover Institution. He joined the Stanford faculty in 1995. He is also an analyst for NBC News and a contributing columnist to *The Washington Post*.

Mike Rogers

Mike Rogers is a former member of Congress, officer in the Army, and FBI special agent. In the U.S. House he chaired the Intelligence Committee, becoming a leader on cybersecurity and national security policy, and overseeing the 17 intelligence agencies' $70 billion budget. Today Mike is a CNN national security commentator, and hosts and produces CNN's "Declassified." He serves as Chief Security Adviser to AT&T, sits on the board of IronNet Cybersecurity and MITRE Corporation, and advises Next Century Corporation and Trident Capital. He is Distinguished Fellow and Trustee at Center for the Study of the Presidency and Congress, and a Senior Fellow at the Belfer Center at Harvard University.

Kori Schake

Kori Schake has served in various policy roles including at the White House for the National Security Council, at the Department of Defense for the Office of the Secretary and Joint Chiefs of Staff, and at the State Department for the Policy Planning Staff. During the 2008 presidential election, she was senior policy advisor on the McCain–Palin campaign. She is now a research fellow at the Hoover Institution. She is the editor, with Jim Mattis, of the book *Warriors and Citizens: American Views of Our Military*. She is the Deputy Director-General at the International Institute for Strategic Studies, a contributing editor covering national security and international affairs at *The Atlantic*, a columnist for *Foreign Policy* magazine, and a contributor to *War on the Rocks*.

Julie Smith

Julianne "Julie" Smith served as the deputy national security advisor to the U.S. vice president from 2012 to 2013, acting national security advisor to the vice president in 2013, and principal director for European and NATO policy in the Office of the Secretary of Defense in the Pentagon. Smith is currently senior fellow and director of the Transatlantic Security Program at the Center for a New American Security.

Admiral Jim Stavridis (Ret.)

Admiral James Stavridis, U.S. Navy (Ret.) served as commander of European Command and as Supreme Allied Commander, Europe from 2009 to 2013. He commanded U.S. Southern Command in Miami from 2006–09 and commanded Enterprise Carrier Strike Group, conducting combat operations in the Arabian Gulf in support of both Operation Iraqi Freedom and Operation Enduring Freedom from 2002–04. He was a strategic and long-range planner on the staffs of the Chief of Naval Operations and the Chairman of the Joint Chiefs of Staff. He has also served as the executive assistant to the secretary of the navy and as senior

military assistant to the secretary of defense. He is now dean of the Fletcher School of Law and Diplomacy, Tufts University, and chairman of the U.S. Naval Institute board of directors.

Jake Sullivan

Jake Sullivan served in the Obama administration as national security advisor to Vice President Joe Biden and director of Policy Planning at the U.S. Department of State, as well as deputy chief of staff to Secretary of State Hillary Clinton. He was the senior policy advisor on Secretary Clinton's 2016 presidential campaign. He is now a senior fellow at the Carnegie Endowment for International Peace and Martin R. Flug visiting lecturer in law at Yale Law School.

Nicole Wong

Nicole Wong served as deputy U.S. chief technology officer in the Obama administration, where she focused on internet, privacy, and innovation policy. Prior to her time in government, Nicole was Google's vice president and deputy general counsel, and Twitter's legal director for products. She frequently speaks on issues related to law and technology. Nicole chairs the board of Friends of Global Voices, a nonprofit organization dedicated to supporting citizen and online media projects globally. She also sits on the boards of WITNESS, an organization supporting the use of video to advance human rights, and the Mozilla Foundation, which promotes open internet. Nicole currently serves as an advisor to the School of Information at the University of California, Berkeley, Harvard Business School Digital Initiative, the Democratic National Committee Cybersecurity advisory board, Refactor Capital, and the Albright Stonebridge Group.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org

Chairman BURR. Ms. Rosenberger, thank you.
Dr. Howard.

STATEMENT OF PHILIP HOWARD, Ph.D., DIRECTOR, OXFORD INTERNET INSTITUTE

Dr. HOWARD. Thank you, Chairman Burr and Vice Chairman Warner, for the opportunity to testify on foreign influence operations and their use of social media platforms.

My name is Phil Howard. I'm a professor at Oxford University and Director of the Oxford Internet Institute, a department at Oxford. My own area of expertise includes political communication and international affairs. And at the institute, I've been leading a project on computational propaganda, currently funded by the European Research Council, and something that—a research initiative that started with support from the National Science Foundation in this country.

I began working on these questions in 2010, but the project really grew in the summer of 2014, when the Malaysian Airlines flight was shot down over Ukraine. And in Hungary, where I was based at the moment, at that time, many of my Hungarian friends got multiple ridiculous stories about what had happened. We knew these came from Russian or Russian sources.

There was one story that democracy advocates had shot the plane down because they thought Putin was traveling on commercial from Amsterdam to Malaysia. There was another story that Americans had shot the plane down because the U.S. had stationed troops in Ukraine. And far and away my favorite was the story of a lost tank from World War II that had come out of the great forests of Ukraine that was confused and had shot the plane down.

It was at that moment that we realized the thrust of Russian propaganda was not so much about creating one counter-narrative and placing that story amongst a public, but creating multiple, sometimes equally ridiculous, stories and placing those stories in a public. What we did not expect is that Russia would turn this campaign strategy on America, on the other great democracies in the West.

I'm going to say a little bit about what we've learned over the last few years about the form of these computational propaganda campaigns and give you a sense of what I expect for 2018 and perhaps the years ahead.

We coined the term "computational propaganda" because this kind of disinformation is unique. It makes use of automation; it makes use of the social media algorithms that technology firms themselves have built. And it makes use of those algorithms to distribute targeted propaganda. This propaganda includes falsely packaged news, misinformation, illegal data harvesting, hacking. There's a range of techniques that goes into backing computational propaganda.

And there's three kinds of campaigns that tend to target voters. There are campaigns to polarize voters on particular issues. For example, known Russian social media accounts will simultaneously promote political action by groups like the United Muslims of America and the Army of Jesus, or encourage African-American political activity around Black Lives Matter and encourage others to

support the Blue Lives Matter movement. The goal is to get groups of voters to confront each other angrily, not just over social media, but in the streets.

Second, there are campaigns to promote or discredit particular senators, presidential candidates and other political figures. Foreign-backed rumormongering is not new, but it is strategically targeted in a way that is new.

Third and perhaps most worrying for democracy is that campaigns, some of these campaigns, discourage voters from voting. Voter suppression is a common messaging technique aimed at voters whose support for a candidate a foreign government might find unpalatable. For example, voters are often told that voting day has been postponed, or that they can text message their vote in, or that the polling station has moved when it has not.

In the case of the United States, these campaigns are ongoing. Months after the last major election in the U.S., our team demonstrated that disinformation about national security issues, including information from Russian sources, was being targeted at U.S. military personnel, veterans and their families.

During the President's State of the Union Address, we demonstrated that junk news, some of which originates from foreign governments, is particularly appetizing for the far right, white supremacists, and President Trump's supporters, though notably not small "c" conservatives.

Our team has completed recently a global inventory of the number of governments managing these campaigns and, while many of us talk about Russia, I would say that the original writ of our research was to track what the Russians and Chinese are doing in this domain. So far, we have not documented much Chinese activity. We know they spend time working on voters in Taiwan, they work on the Chinese diaspora. We believe they have capacity, but as of yet they haven't set American voters in their sights.

We have found in this most recent inventory that there are 48 countries in the world with large political parties or government agencies running misinformation campaigns either on their own voters or on voters in other countries. There are seven authoritarian governments, aside from Russia, that spend money in this domain.

And overall, I would say it's time for democracies to develop their own cyber-security strategies. The time for industry self-regulation has probably passed. And I'm grateful for this opportunity to discuss the possibilities going forward.

[The prepared statement of Dr. Howard follows:]

Testimony of Philip N. Howard, Oxford University

"Foreign Influence on Social Media Platforms: Perspectives from Third-Party Social Media Experts"

Senate Select Committee on Intelligence, Open Hearing, August 1, 2018

Thank you, Chairman Burr and Vice Chairman Warner, for the opportunity to testify on foreign influence operations and their use of social media platforms.

My name is Phil Howard; I am a Professor at Oxford University and Director of the Oxford Internet Institute, an academic department of Oxford University. My areas of expertise include political communication and international affairs.

There is a significant amount of punditry and speculation about the role and impact of foreign influence operations and their use of social media platforms. I tend to work with open-source information, public archives, and the feeds of data that the social media platforms make available. I think I can best serve you by sticking close to evidence that has either come (1) from my own research team at Oxford University or (2) from the network of academics who are evaluating foreign influence on social media platforms.

OUR RESEARCH FINDINGS

At the Oxford Internet Institute, I have been leading the Project on Computational Propaganda, which is currently funded by the European Research Council. I began working on this in 2010 with the support of the National Science Foundation, and our research team was the first large-scale, dedicated effort to study the role of disinformation and social media manipulation in public life.

We coined the term "computational propaganda" because this kind of disinformation is unique: it makes use of automation, algorithms and big-data analytics to manipulate public opinion in targeted ways.[1] The term encompasses political content falsely packaged as news, the spread of misinformation on social media platforms, illegal data harvesting and micro-profiling, the exploitation of social media platforms for foreign influence operations, the amplification of hate speech or harmful content through fake accounts or political bots, hacking and social engineering, and clickbait content for optimized social media consumption. Computational propaganda is often illegal under the existing rules of elections administration that most democracies have in place.[2]

---

[1] Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents — Introduction," *International Journal of Communication*, Automation, Algorithms, and Politics Special Section, 10, no. 0 (2016): 9.

[2] Philip N. Howard, Samuel Woolley, and Ryan Calo, "Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration," *Journal of Information Technology & Politics* 15, no. 2 (April 3, 2018): 81–93, https://doi.org/10.1080/19331681.2018.1448735.

Based on publicly available data, including the small amounts of data that the social media firms released last summer, there are several things we know about the strategies that Russian operators employ and which US voters they seek to influence. Our team has worked with data on the accounts that the social media platforms have exposed as managed by Russian operators. We know what messages these accounts sent and what advertisements these users bought and then targeted at US voters.

From this evidence, we can identify several kinds of computational propaganda campaigns.

1. *Campaigns to polarize voters on particular issues*. For example, known Russian social media accounts will simultaneously promote political action by a group called "United Muslims of America" and the "Army of Jesus", or encourage African American political actives around "Black Lives Matter" and then develop a "Blue Lives Matter" movement. The goal is to get groups of voters to confront each other angrily, over social media and in the streets. Video content, edited and taken out of context, makes new immigrants seem like a threat to veterans, or tells one community that the police need our support while telling another that police are abusing them.
2. *Campaigns to promote or discredit particular Senators, Presidential candidates, and other public figures*. Foreign-backed rumor-mongering is not new, but it is much more strategically targeted within districts and by voter demographics than before. It is safe to say that every public figure on the national stage is either attacked by or benefits from highly automated or fake social media accounts, and whether these campaigns are managed by foreign governments depends on the issues involved and time of the campaign season.
3. *Campaigns to discourage citizens from voting.* Voter suppression is a common messaging strategy, aimed at the voters who might support a candidate that a foreign government finds unpalatable. For example, voters are often told that voting day has been postponed, or that they can text message their vote in, or that their polling station has moved.

It is difficult to know how many people in the United States have seen such messages, or how many voters were actually influenced by them. Only the social media firms themselves could share that data or estimate those probabilities accurately. But, in the US context, it is safe to assume that social media platforms efficiently delivered these messages and advertisements to voters, and that these messages had an influence, in different ways, in different states, and in conjunction with all the other variables that shape an electoral outcome.

THE UNITED STATES AS A TARGET

We have demonstrated that, during the last Presidential election, there was a one-to-one ratio of junk news to professional news shared by voters over Twitter. In other words, for every one link to a story produced by a professional news organization there was one link to content that was extremist, sensationalist, conspiratorial or other form of junk news. Not only is this the highest level of junk news circulation in any of the countries we have studied, but this misinformation was actually concentrated in swing states.[3] Disinformation campaigns are often launched with highly automated accounts and fake users, and these kinds of accounts pushed significant amounts of content from Russian news sources, links to unverified content on WikiLeaks, and other junk news. Our analysis demonstrates that this

[3] P N. Howard et al., "Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?," Data Memo 2017.8 (Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, 2018).

content does not simply flow across networks of bots—at the right volume level it can permeate deeply into networks of human users.[4]

These operations are ongoing. Months after the last major election in the US, we demonstrated that disinformation about national security issues, including from Russian sources, was being targeted at US military personnel, veterans, and their families.[5] During the President's State of the Union address, we learned that junk news is particularly appetizing for the far right, white supremacists, and President Trump's supporters (though not "small c" conservatives).[6] Some of this junk content actually originates with accounts managed by foreign governments.

INFLUENCE OPERATIONS GLOBALLY

Our team recently completed a second global inventory of the organizational capacity of different governments and political parties to manipulate public opinion over social media. Around the world, a range of government agencies and political parties are exploiting social media platforms to spread junk news and disinformation, exercise censorship and control, and undermine trust in the media, public institutions, and science. At a time when news consumption is increasingly digital, artificial intelligence, big-data analytics, and "black-box" algorithms are being leveraged to challenge truth and trust. These are cornerstones of democracy.

In 2017, our first global cyber troops inventory shed light on the global organization of social media manipulation by government and political party actors.[7] Now, only a year later, we find a significant expansion of this capacity.[8]

1. We have found evidence of formally organized social media manipulation campaigns in 48 countries, up from 28 countries last year. In each country, there is at least one political party or government agency using social media to manipulate public opinion domestically.
2. Much of this growth comes from countries where political parties are spreading disinformation during elections, or countries where government agencies feel threatened by junk news and foreign interference and are responding by developing their own computational propaganda campaigns in response.

---

[4] Samuel Woolley and Douglas Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online," Working Paper 2017.5 (Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, June 2017).
[5] John Gallacher et al., "Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans," Data Memo 2017.9 (Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, March 26, 2017).
[6] Vidya Narayanan et al., "Polarization, Partisanship and Junk News Consumption over Social Media in the US," Data memo 2018.1 (Oxford, United Kingdom: Oxford Internet Institute, University of Oxford, June 2017).
[7] Samantha Bradshaw and Philip N. Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," Working Paper 2017.12 (Oxford, England: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, July 2017), http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.
[8] Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Working Paper 2018.1 (Oxford, England: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, July 2018), http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.

3. In a fifth of these 48 countries—mostly across the Global South—we found evidence of disinformation campaigns operating over chat applications such as WhatsApp, Telegram and WeChat.
4. Computational propaganda still involves social media account automation and online commentary teams, but is making increasing use of paid advertisements and search engine optimization on a widening array of Internet platforms.
5. Social media manipulation is big business. Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media. In a few countries this includes efforts to counter extremism, but in most countries this involves the spread of junk news and misinformation during elections, military crises, and complex humanitarian disasters.

RESEARCH ON VOTER IMPACT

Some of the best evidence about social media advertising and influence comes from the platforms themselves. A growing number of researchers work with social media data over polling data to answer basic research questions about public opinion dynamics.[9] Social media are not only important for obtaining news and political content, but also as an indicator of public sentiment in elections and other political crises.[10] No matter the platform, social media users are producing a vast amount of data that is collected and analyzed to generate detailed psychological profiles of users that can provide insight into attitudes, preferences, and behaviors. Indeed, the successful business model of these firms is to algorithmically connect users to content that is relevant to them individually, as well as target them with personalized advertising, using systems that political actors can "pay to play" in. The information users produce about themselves online helps craft the computational propaganda they are subsequently sent, influencing voting behavior and improving voter turnout.[11] The study of news consumption habits of social media users can also produce fine- grained analyses of the causes and consequences of political polarization.[12]

Social media almost certainly facilitates selective exposure, but more likely through *social* endorsements rather than simply partisan frames. On Facebook, friends share news from consistent ideological perspectives, rarely using diverse sources of political news and information. In a study by Bakshy et al., Facebook users encountered roughly 15% less cross-cutting content in their news feeds due to algorithmic ranking, and clicked through to 70% less of this cross-cutting content.[13] Within the domain of political news encountered in social media, selective exposure appears to drive attention. However, the underlying driver of attention is the social endorsement that is communicated through the act of sharing: social media users will not pay attention simply because a piece of political news is from a

[9] Robert Bond and Solomon Messing, "Quantifying Social Media's Political Space: Estimating Ideology from Publicly Revealed Preferences on Facebook," *American Political Science Review* 109, no. 01 (2015): 62–78.
[10] Daniel Gayo-Avello, "A Meta-Analysis of State-of-the-Art Electoral Prediction from Twitter Data," *Social Science Computer Review*, 2013, 0894439313493979, https://doi.org/10.1177/0894439313493979.
[11] Robert M. Bond et al., "A 61-Million-Person Experiment in Social Influence and Political Mobilization," *Nature* 489, no. 7415 (September 13, 2012): 295–98, https://doi.org/10.1038/nature11421; Michael Brand, "Can Facebook Influence an Election Result?," The Conversation, 2016, http://theconversation.com/can-facebook-influence-an-election-result-65541; Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111, no. 24 (2014): 8788–90, https://doi.org/10.1073/pnas.1320040111.
[12] Eytan Bakshy, Solomon Messing, and Lada A. Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook," *Science* 348, no. 6239 (June 5, 2015): 1130–32, https://doi.org/10.1126/science.aaa1160.
[13] Bakshy, Messing, and Adamic.

credible source or generated by a political party, they pay attention because someone in their social network has signaled the importance of the content.[14] Other researchers have found that when the top search results about a political leader are positive, people say they will vote for that person. When they are shown negative results, people report that they less likely to vote.[15] So it should not be surprising that foreign governments seeking to interfere with domestic politics and shape public opinion inside a country would put resources into manipulating search results.

CONCLUSION: WHAT IS NEXT?

Disinformation campaigns will continue to be launched against voters in democracies. For every new social media platform, every new design idea on every platform, and every new digital device, someone will work to integrate the innovation with a computational propaganda campaign.[16]

First, globally, we can expect a growing number of foreign powers to develop disinformation campaigns for single issues and legislative campaigns, not just elections.

Second, globally, we can expect foreign governments to apply these techniques and develop these messages for multiple platforms. They will to whatever social media platform has voters.

Third, globally, we can expect advances in artificial intelligence and machine learning to be used to support ever more individuated campaigns. Currently, foreign influence operations take advantage of the algorithms built by social media firms and search engines to customize the delivery of disinformation. Artificial intelligence, machine learning, and natural language processing will not only be used for individual targeting, but individually customized content. Videos and text can be crafted by knowledge of credit card purchases, and device data from our mobile phone, or from our "Internet of Things" refrigerator.

Fourth, globally, we can expect regimes other than Russia to develop their capacity to influence domestic public opinion. We believe China has significant capacity, but have only caught their influence operations against Taiwan and the Chinese diaspora. Authoritarian governments tend to learn from each other, and we have seen more and more such regimes applying these techniques.

Fifth, within the United States, we can expect the same kinds of voters to continue to be targets for misinformation. Given the disinformation campaigns which have been—and are currently— running, I would guess that foreign actors will continue to aim future disinformation campaigns at African American voters, Muslim American voters, White Supremacist voters, and voters in Texas and the Southern States. I expect the strategy will remain the same: push disinformation about public issues; discredit politicians and experts; and prevent particular types of voters from participating on Election Day.

---

[14] Bakshy, Messing, and Adamic; Solomon Messing and Sean J. Westwood, "Selective Exposure in the Age of Social Media: Endorsements Trump Partisan Source Affiliation When Selecting News Online," *Communication Research* 41, no. 8 (2014): 1042–63, https://doi.org/10.1177/0093650212466406.

[15] Robert Epstein and Ronald E. Robertson, "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections," *Proceedings of the National Academy of Sciences* 112, no. 33 (August 18, 2015): E4512–21, https://doi.org/10.1073/pnas.1419828112.

[16] Philip N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (New Haven, CT: Yale, 2015).

The manipulation of public opinion over social media platforms has emerged as a critical threat to public life. The solution to these problems necessarily involves research and public policy oversight. Technology firms occasionally share small amounts of data, but providing a regular flow of data about public life to elections administrators, researchers, and civil society groups is the best way to ensure that social media firms make good decisions and design their platforms to support and defend, rather than undermine and expose, our democratic institutions.

REFERENCES

Bakshy, Eytan, Solomon Messing, and Lada A. Adamic. "Exposure to Ideologically Diverse News and Opinion on Facebook." *Science* 348, no. 6239 (June 5, 2015): 1130–32. https://doi.org/10.1126/science.aaa1160.

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489, no. 7415 (September 13, 2012): 295–98. https://doi.org/10.1038/nature11421.

Bond, Robert, and Solomon Messing. "Quantifying Social Media's Political Space: Estimating Ideology from Publicly Revealed Preferences on Facebook." *American Political Science Review* 109, no. 01 (2015): 62–78.

Bradshaw, Samantha, and Philip N. Howard. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." Working Paper 2018.1. Oxford, England: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, July 2018. http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.

———. "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation." Working Paper 2017.12. Oxford, England: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, July 2017. http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.

Brand, Michael. "Can Facebook Influence an Election Result?" The Conversation, 2016. http://theconversation.com/can-facebook-influence-an-election-result-65541.

Epstein, Robert, and Ronald E. Robertson. "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections." *Proceedings of the National Academy of Sciences* 112, no. 33 (August 18, 2015): E4512–21. https://doi.org/10.1073/pnas.1419828112.

Gallacher, John, Vladimir Barash, Philip N. Howard, and John Kelly. "Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans." Data Memo 2017.9. Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, March 26, 2017.

Gayo-Avello, Daniel. "A Meta-Analysis of State-of-the-Art Electoral Prediction from Twitter Data." *Social Science Computer Review*, 2013, 0894439313493979. https://doi.org/10.1177/0894439313493979.

Howard, P N., Bence Kollanyi, Samantha Bradshaw, and Lisa-Maria Neudert. "Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?" Data Memo 2017.8. Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, 2018.

Howard, Philip N. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven, CT: Yale, 2015.

Howard, Philip N., Samuel Woolley, and Ryan Calo. "Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration." *Journal of Information Technology & Politics* 15, no. 2 (April 3, 2018): 81–93. https://doi.org/10.1080/19331681.2018.1448735.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *Proceedings of the National Academy of Sciences* 111, no. 24 (2014): 8788–90. https://doi.org/10.1073/pnas.1320040111.

Messing, Solomon, and Sean J. Westwood. "Selective Exposure in the Age of Social Media: Endorsements Trump Partisan Source Affiliation When Selecting News Online." *Communication Research* 41, no. 8 (2014): 1042–63. https://doi.org/10.1177/0093650212466406.

Narayanan, Vidya, Vladimir Barash, John Kelly, Bence Kollanyi, Lisa-Maria Neudert, and Philip N. Howard. "Polarization, Partisanship and Junk News Consumption over Social Media in the US." Data memo 2018.1. Oxford, United Kingdom: Oxford Internet Institute, University of Oxford, June 2017.

Woolley, Samuel C., and Philip N. Howard. "Political Communication, Computational Propaganda, and Autonomous Agents — Introduction." *International Journal of Communication*, Automation, Algorithms, and Politics Special Section, 10, no. 0 (2016): 9.

Woolley, Samuel, and Douglas Guilbeault. "Computational Propaganda in the United States of America: Manufacturing Consensus Online." Working Paper 2017.5. Oxford, United Kingdom: Project on Computational Propaganda, Oxford Internet Institute, Oxford University, June 2017.

Chairman BURR. Dr. Howard, thank you very much.

I am reminded, after listening to all of the testimony, that the 1960s strategies of Russia were simple: If it's bad for America, it must be good for us. And it seems like this is rooted in the same foundational strategic vision that they had then.

The Chair would recognize himself for five minutes. I'm going to ask all of you to follow my chart over there. I just want to get your comments relative to whether this is accurate or not.

[The material referred to appears in the Supplemental Material on page 163.]

Chairman BURR. The red line represents the Russian activities of the IRA Twitter activity relative to outside the United States. The blue line is U.S.-focused IRA Twitter activities. What that shows is a huge spike up in the 2014–2015 timeframe, which was the invasion of the Ukraine.

The next two jogs of the lineup are between 2015 and 2016, and that's the Crimea propaganda, and the regional politics in Belarus specifically.

And then all of a sudden you see this spike in the blue line in the United States. I think the fascinating thing here is that the spike is in 2017 and 2018, which tells us—and correct me if I'm wrong—the effort in 2017 and 2018 was much more intense than the effort in 2015 and 2016 in the lead-up to an election. Am I misreading that?

[No response.]

So, Dr. Kelly, let me ask you this: Is it possible for the mainstream media today to run a story that was the creation of an effort by the IRA, that had no factual basis, but over the transition of how their strategies work, it gained enough coverage, belief that people had read it, that it got so big that it had to have been real? Is that possible?

Dr. KELLY. I believe it is possible. I think the goal of these information operations over the long term is to condition the public and to weave the network, so to speak, that later you can use it to move any sort of story.

Remember, a key feature of propaganda—you know, if you're running a propaganda outfit, most of what you publish is factual, so that you're taken seriously, and then you can slip in the wrong thing at exactly the right time. I believe that's what they've done, is cultivate a set of sources as authoritative with content that's often just about Kim Kardashian. And then those people become credible, they become cited in the mainstream media. And then at that point, they can start to move anything they want through it.

Chairman BURR. And is it the individuals that contribute to that theme that's on a social media platform, in many cases Americans responding, that gives it credibility? And are they knowing or unknowing as to what they're participating in?

Dr. Helmus, have you got a strategy on that?

Dr. HELMUS. Certainly I agree that there's no borders on social media. There's no borders on media today. So certainly content that's disseminated by one source could easily get picked up by another. It's our observation from looking at Eastern Europe that there's fundamental issues with journalism training and quality that can certainly lead to and exacerbate that type of issue of, you

know, bringing viral content that is otherwise false or untrue into perceptions of reality.

Chairman BURR. Ms. DiResta, you said, and correct me if I'm wrong, IRA pages stay active today.

Ms. DIRESTA. Yes, sir, I believe that's true; and Twitter accounts that were associated with IRA botnets also appear to be dormant today with the potential to be able to be turned back on at some point.

Chairman BURR. So with all the efforts by the Justice Department at targeting by the public acknowledgement and indictment of individuals, the IRA has not gone away?

Ms. DIRESTA. No, sir.

Chairman BURR. Their capabilities—and comment on it if you will—their capabilities relative to Facebook's latest disclosure may have gotten significantly better.

Ms. DIRESTA. One thing that's a very big, significant challenge is attribution. So we can attribute this to the IRA, perhaps. I also read the same news that you read yesterday and don't have any inside information there. My understanding is they believe it was the IRA based on image similarities, tactical similarities.

What they did change was they paid in, I believe, U.S. dollars and Canadian dollars. So they are no longer paying in rubles. They are probably no longer using IP addresses that are tied to Russia; slight increases in operational security that will make them more difficult to detect.

The other thing that is going to go along with that, though, is as attribution is so difficult, particularly for outsiders who don't have access to that kind of account level, what we call metadata, is that other people will be able to run the same playbook, perhaps making it look like an IRA operation when it was conducted domestically.

Chairman BURR. Individual or a nation state?

Ms. DIRESTA. Individual or nation state, yes, sir.

Chairman BURR. Great, thank you.

Vice Chairman.

Vice Chairman WARNER. Thank you all for your testimony. I think a couple of things. One, we're still mostly just talking about the IRA activity, as opposed to what we don't know in terms of other Russian services' activities. And we do know the IRA, with the revelations of yesterday, has gotten better.

And we're going to still need to figure out their tradecraft. And one of the things we need from expertise like you is I feel like even when the platform companies are moving in the right direction, they're only doing it looking at their own universe, their own platform, not the interrelationship.

I think, Mr. Kelly, you said something that was maybe the single most stunning line of all the testimony, that in terms of the political content, particularly on the extremes, that 25 to 30 times more of that content is being generated by bots and automated accounts rather than individuals. Is that correct?

Dr. KELLY. Yes, Senator, that's correct. If you look at the American political spectrum and, say, array a set of politically oriented Twitter accounts along an axis where on one side you've got those that only talk to people of their own, you know, stripe, and on the

other it's the other stripe, and most Americans are in between, connected to some on the right and the left, those on the either extreme of that network are shouting with automated amplification.

Vice Chairman WARNER. So with a lot of that automated.

Let me state for the record, we had some of this—I've had conversations with you in the past. There are very appropriate and effective roles for automated accounts and bots in certain cases. But I guess what I would ask—I'll start with Ms. Rosenberger and Dr. Kelly on this: Shouldn't we as human beings have a right to know—maybe not make a judgment, but a right to know whether the content that we're receiving is coming from a human being versus an automated account; recognizing that there is good value in some of the automated accounts?

Ms. ROSENBERGER. Yes, Senator. I believe that context about information is absolutely critical for consumers of that information to be able to evaluate it. When we talk about critical thinking in media literacy, this takes on wholly new characters when we talk about online content. And so having information about the origin of information, about whether or not that content is being served up through an automated process, why users are seeing that kind of information, I absolutely believe that's critical.

One thing I do think is important in this conversation is that we ensure we protect the anonymity online, which is essential for democratic activists in authoritarian states. But I believe very deeply that there are ways to identify automation without compromising the ability for users, real users, to be anonymous.

Vice Chairman WARNER. Dr. Kelly, do you want to?

Dr. KELLY. Well, we have to recognize that automation is performing a lot more functions online that simply supporting Russian propagandists. And the fact that it's doing so many different things, some of which are, you know, call them green things we like and some of which are red things we don't like, makes it extremely hard, without being able to know who's running that robot, to know who's using it for good or bad.

Vice Chairman WARNER. Dr. Howard, did you want to weigh in on this?

Dr. HOWARD. No.

Vice Chairman WARNER. Could we analogize to the markets where, with the huge advances around HFT and high frequency traders—the markets, in terms of trying to make sure that things didn't get totally away, put certain speeds bumps in place. And if the market jolts one way or another, there are these speed bumps that then allow in a sense human activity.

With the, again, 25 to 30 times automation, if there are stories that are trending at an enormously rapid rate, that might be trending because they've got this enormous amount of automation driving that story, you know, could there be some kind of time out so that you could, a company, or some entity, could evaluate whether this is actual, not actual? Something looks phony here, fishy here? Any of you on that comment?

Ms. DIRESTA. I think that the parallel to HFT is spot on. I think that it's an issue of information integrity. And one of the challenges that the platforms have had is believing that they need to address

the core of the narrative. And what we should be looking for is addressing the dissemination patterns that you're mentioning.

Vice Chairman WARNER. I think that's really—go ahead, Mr. Kelly.

Dr. KELLY. Well, one thing to keep in mind is that, again, automation is running all kinds of things. So it's not just pushing Russian propaganda. It's pushing legitimate American political speech. It's also pushing pop music elements in, you know, marketing around music. So automation is doing a lot of things in different places.

Vice Chairman WARNER. And I'll make the comment that it doesn't come with good or bad attached. But I guess I just think as a human being, I ought to have that knowledge of whether that message is being promoted to me by a human being or by automation.

And I know my time's up. I just want to come back, asking Ms. Rosenberger on the next round of, you know, could we deal with that protection of anonymity, but still put some geocoding so that if somebody says Richard Burr from North Carolina, but it's actually come from a different location?

Thank you, Mr. Chair.

Chairman BURR. Dr. Howard, did you have something you wanted to add to that?

Dr. HOWARD. I just wanted to add that the other possibility is to have these accounts self-identify with B–O–T, bot, in the name. That kind of disclosure is what helps users separate the good content from the bad.

Chairman BURR. Great.

Senator Risch.

Senator RISCH. Well, thank all of you for coming here today.

I think the takeaway from this, after listening to all of this, is something that's troubled me from the beginning and that is how difficult this is. We know the problem. We have bad actors putting out bad information. The difficulty is how do you segregate those people who are doing this from Americans who have the right to do this?

I've looked at the stuff that—that, as everybody has, that is part of this. But yet, if you took one of those pieces, any one of them individually, and looked at it and said, we just discovered who's doing this, it's John Doe in East Overshoe, New Jersey, there's nothing illegal about it. It may be disgusting. It may be untrue. It may be with a bad motive. But there's nothing—indeed, it's protected by the First Amendment of the Constitution.

So how do you separate that person from someone who is doing the same thing, but coming from Russia, but whose motives are to enhance Russia by pulling down America? How do you police that?

And I think, probably, the question that Senator Warner asked about putting a speed bump in so that somebody can evaluate this. I mean, that kind of puts—I want to be the evaluator, and I think most everybody does, and that's the problem.

And then you talked about protecting anonymity. How do you—how can you protect anonymity if you're going to actually do something against someone who is doing something that we don't want done?

These are extremely difficult questions. And I appreciate all the kind things you've said about this is bipartisan, we all need to come together, et cetera, et cetera. We all agree with that, but how in the world do you do this? I mean, the takeaway here has got to be that this is just an enormous, if not an impossible, thing.

Mr. Helmus, your thoughts?

Dr. HELMUS. Yes, I absolutely agree. I think that is the fundamental question.

In our research, we identified upwards of 40,000 accounts centered around Ukraine that are putting out vociferously anti-Ukraine content. And ultimately, the crux is are these bad actors that are doing this? Or is this a free—other actors practicing what might otherwise be their free speech?

So, that's challenged our bot detectors. So, there are some ways, and I'll defer to others on the Committee who can speak to these, but there are bot detectors that are available that can detect some types of content that mimic the characteristics of bots. But it is an arms race. As developers develop ways to detect bots based on either inhuman levels of content, the timing of their tweets, or what have you, the producers of those bots will then identify other ways of circumventing that and staying covert. So, it's an arms race and I think it will just require constant research and evaluation to develop and update new techniques.

Senator RISCH. Ms. DiResta.

Ms. DIRESTA. What you're describing is a significant problem for researchers as well. And we look at information operations, trying to gauge, again, attribution or whether this is organic or not.

Senator RISCH. But what do you do about it when you do get the attribution?

Ms. DIRESTA. We try to look at the content. Has it appeared elsewhere? Is it affiliated with past IRA operations? Or is it coming from somewhere else? So, we look at the origin.

We look at the voice; the actors that are pushing the content. Are they bots? Are they humans? Is there something off about the bio related to past tweets? There's a number of signatures there. And then, we look at the dissemination pattern. Does it look like it's been artificially amplified? Is it being run through accounts, or groups, or pages that seem a little bit dubious?

We try to flag things for the social platforms as well. We believe firmly in transparent communication, where we're saying, this is what we're seeing, what are you seeing? They have access to metadata and to account information and to e-mail addresses, phone numbers, things that people have registered their accounts with. That is also a significant part of the investigation of the operation.

There is no easy answer to this question. This is the primary challenge and this is where we see even influence operations going towards laundering narratives, either through the unwitting or through participants. That's a hard problem.

Senator RISCH. The analysis that you're talking about is you're looking for all of these things. But you'll find, I assume, some actors that are, what we would consider, bad actors, but yet, some actors that we would consider good actors, whether it was a U.S. government operation or something.

Who makes the determination as to who's a good actor and a bad actor? That's what I really, really struggle with.

Ms. DIRESTA. And I think the——

Senator RISCH. Dr. Kelly, why don't you get your two cents worth in?

Dr. KELLY. Thank you, Senator.

So it's tractable to tell what's fake. It's harder, but doable, to figure out who is behind it. And then you need to understand who's behind it, tracking the landscape of threat actors. That's where somebody is making a determination who's against our interests and who doesn't matter. Then, once you have that, you know, it's up to government and other appropriate folks to figure out the response.

I think to do that detection in the first place requires an enormous amount of data and sophisticated methods of analysis. And it's not just data from one platform, so, it can't happen only internally. It has to happen with data from multiple sources, which then gets to your, I think, extremely important questions about who makes these determinations and who has the right to see that private data.

I think we have to look at a model that's like cyber-security firms. So there are trusted industry partners that everybody trusts, that they know are going to be secure in the way they handle that data. We need some sort of a facility like that where these advanced——

Senator RISCH. Of course, this is different than cyber-security, in that with cyber-security you don't want anybody entering a private space, whereas with this you want everybody entering. That to me differentiates the two.

My time is up. Thank you, Mr. Chairman. Thank you.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks, Mr. Chairman.

I want to thank Facebook for their move yesterday to delete 32 pages and 290,000 accounts on the basis that Russia and other outside actors are continuing to weaponize social media platforms. I'm very pleased that Facebook took this action, and I hope that all social media platforms continue to actively counter Russia's foreign influence campaign. I have no question that it's going on, and I have no question that it is related to more than just election interference.

Let me ask this question: Since the 2016 election ended, how many IRA accounts have any of you found that are still active?

Dr. Kelly.

Dr. KELLY. We've been doing some work on this. We went and looked—I mean, that list of accounts is extremely valuable. We looked for live accounts on other platforms using open source research tools and we found a great deal of accounts directly connected to the closed accounts, which were active across numerous platforms.

Senator FEINSTEIN. Can you put a number on it?

Dr. KELLY. Of the sample we've looked at so far, it's roughly 28 percent of those accounts are connected to at least one live account on a different platform. We also know that those accounts were connected to numerous other Twitter accounts and where—we

think of this as what we have here is the tentacle of an octopus, and we don't know how far out on the arm of that octopus that tentacle has gotten.

Senator FEINSTEIN. How about Russia's accounts?

Dr. KELLY. The Russian accounts evident in this data?

Senator FEINSTEIN. Right.

Dr. KELLY. Well, presumably these are IRA accounts too and presumably they have their own—you know, they've got a tentacle wagging in Russia as well and I don't know how much of their effort this represents.

Senator FEINSTEIN. Does anybody else on the panel have a comment on this subject matter?

Yes. Please, doctor?

Dr. HOWARD. Thank you, Senator. My comment would be that it's the social media firms who have that information. We do our best juggling probabilities and percentages to make best guesses about what kinds of account. Some of these accounts occasionally slip into Cyrillic and then slip back. There are some giveaways. But it's actually the social media firms that have the best data on this.

Senator FEINSTEIN. Well, let me ask you this question. Facebook has alleged that IRA activity on its platform alone reached 126 million people and that doesn't include Instagram or Twitter. What can you say about the extent to which the IRA activity reached real Americans?

Dr. HOWARD. I can say that it was significant, yet also concentrated in swing states.

Senator FEINSTEIN. I'm sorry? Concentrated in?

Dr. HOWARD. Swing states——

Senator FEINSTEIN. Swing states.

Dr. HOWARD [continuing]. During the 2016 election. So particular states got more of this kind of content than other states.

Senator FEINSTEIN. And what was the time that you looked at that to draw that conclusion?

Dr. HOWARD. It was from the beginning of the presidential debates until through to a few days after Election Day.

Senator FEINSTEIN. Have you looked at it now?

Dr. HOWARD. Not in the last few months, no.

Senator FEINSTEIN. Can you estimate the number of Americans touched by Russian-linked activity in this area?

Dr. HOWARD. No. That is very difficult to do.

Senator FEINSTEIN. Can anybody?

Yes, please go ahead.

Ms. ROSENBERGER. No, I just wanted actually to add a small data point to this, which is we spend a lot of time talking about Facebook and Twitter but as Renee highlighted and others have noted, this is a problem of the entire information ecosystem. This is cross-platform. Reddit confirmed hundreds of IRA-created accounts. Tumblr did it and in particular on Tumblr, that platform was used to target the African-American community particularly.

So, I think this is why it's so really difficult to quantify in any meaningful way the reach of these activities, because this is across the entire ecosystem, not to mention, as others were highlighting,

how this information gets picked up and then transmitted and amplified through mainstream media outlets.

Senator FEINSTEIN. Let me ask you, when information becomes a weapon, does anybody see any need to change the environment to prevent this from happening?

Ms. DIRESTA. I believe that many of us were advocating doing that when it became clear that ISIS had turned the information ecosystem into a weapon. I believe that, unfortunately, the dialogue between the government, the platforms and researchers was not necessarily where it needed to be. There were a handful of convenings that tried. There was the Global Engagement Center that was established, that's now tied up in some funding morass and we're not really clear what the status of that is.

The tech platforms, about two years after the extent of the ISIS operation became known, established the Global Internet Forum to Counter Terrorism. To the best of my knowledge, that's not staffed so much as it is a repository of hashed content so that platforms can participate in takedowns.

To answer your earlier question with one other point, we did see in the public House data set, when the House released the ads, that the ads were both demographically and geographically targeted. The number of people who saw that content, only the platforms have access to that information, but we could also gauge the number of followers that did follow the Russia pages. And that was in the neighborhood of a couple hundred thousand on the largest pages.

Senator FEINSTEIN. Thanks. My time is up.

Thanks, Mr. Chairman. Thank you.

Chairman BURR. Thank you.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Dr. Kelly, you have a very profound statement in your testimony. You said: Russian efforts are not directed against one election, one party, or even one country. What are Russia's ultimate goals? Is it to undermine the public's faith in Western democracies and so weaken the bonds that unite us, that there are opportunities for Russia?

Dr. KELLY. Yes, Senator, I believe that's exactly correct. I think they have long-term strategic goals, which include weakening Western institutions and faith in democracy and traditional sources of information and authority. That's the strategic goal. And then they have a lot of near, short-term tactical goals, things like injecting hacked information to sway a particular event or election, and they're doing that activity all around their periphery and now here.

Senator COLLINS. Ms. DiResta, this is a question for both you and Dr. Kelly. Both of you emphasized that Russian manipulation did not stop in 2016. In fact, you, Dr. Kelly, said that Russia stepped on the gas and increased its activity. And Ms. DiResta, you said that Russian efforts increased postelection to promote racial tensions in our country.

We imposed sanctions on Russia. They seem to have done no good when it comes to this kind of activity. What can we do beyond educating the public to counter Russia more effectively?

Ms. DiResta, I'll start with you.

Ms. DIRESTA. I would say that one of the things that we need to do is to evaluate our information operations doctrine, JP 313. I believe Senator Warner alluded to this in his recent policy proposals. I think that addressing the scale and sophistication of information operations is something that as a government we've not really looked at that in quite some time and perhaps that would be a good place for us to start.

Senator COLLINS. Thank you.

Dr. Kelly.

Dr. KELLY. I think there's a technical component, which is to be able to effectively detect and attribute this activity so you can authoritatively prove it's happening, and then you have a more traditional toolkit of foreign policy measures to take action.

Senator COLLINS. Dr. Howard, I want to get to something you said, and that was you gave us several compelling examples from your Hungarian experience where they received clearly false stories that were intended to explain the downing of the Malaysian airline. And what's interesting to me is, based on Dr. Kelly's testimony, it isn't just the Hungarian press that is being manipulated or infiltrated or controlled, but we've seen evidence where America's media is also being targeted.

Dr. Kelly pointed out that the Russian persona of Jenna Abrams, who had accounts on multiple platforms, was cited by more than 40 U.S. journalists before being unmasked. How can the media be more sensitive or more aware, more on guard to being manipulated in this way?

Dr. HOWARD. Thank you, Senator. The United States actually has the most professionalized media in the world. It's learned certainly to evaluate their sources and no longer report tweets as given. So I would say that in this country, the most professional news outlets are already on the defense. They already have ways to ensure that the quality of the news product isn't shaped by these constant disinformation campaigns.

I would say that the greater concern would be amongst the media institutions in our democratic allies. I believe that the Russians have moved from targeting us in particular to Brazil and India, other enormous democracies that will be running elections in the next few years. And while we still see significant Russian activity, those countries have the media institutions that need to learn, need to develop.

Senator COLLINS. Ms. Rosenberger.

Ms. ROSENBERGER. Thank you, Senator. I would just add that this is not a problem that we've overcome. We have one example, for instance, of an IRA-created Twitter account, the hash—sorry, the handle was "wokeluisa," that was tweeting in particular to African-Americans, focused on the NFL take-a-knee debate. There were IRA-created accounts tweeting on both sides of that debate. But that Twitter account in particular, which was active through earlier this year, appeared in more than two dozen news stories from outlets such as BBC, USA Today, Time, Wire, The Huffington Post, and BET.

So, this was about four months ago. So, we really do need to make sure that this information is not getting laundered into the broader ecosystem, which is part of the strategy here.

Senator COLLINS. And the issue there is when we read it in a credible source, we're likely to believe it.

Ms. ROSENBERGER. That's exactly right. It gives it that much more credibility.

Senator COLLINS. Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman, and thank all of you.

It seems to me for now and the foreseeable future, protecting America's private data is going to be a national security issue. Cambridge Analytica, like the Russians, exploited Facebook's lax protections to abuse Americans' information. I believe a significant part of the failure is the fact that the Federal Trade Commission doesn't have the authority or the resources to be a tougher cop on the beat. And I'm going to be rolling out a plan to fix that in the weeks ahead.

Now let me go to questions. Ms. DiResta, your testimony referenced the Russian Facebook pages in 2016, targeting both the right and the left. But you noted it was the pages targeting the left that included not only content intended to appeal to its audience, but also content intended to suppress the vote and be critical of Secretary Clinton.

In your view, does the apparent Russian content released yesterday by Facebook resemble the content the Russians used last time to attract an audience on the left and among racial minorities, which the Russians then used to suppress their vote?

Ms. DIRESTA. Yes, sir, it does. There's a strong component of cultural posts that appear in communities and pages targeting minority voters: a lot of pride, pride-related content, less news, more memes and that reflects what we saw yesterday.

Senator WYDEN. I appreciate that, because content targeting I think is clearly going to be a big part of the challenge. The public has got to be aware of it, because not all Russian propaganda is going to get caught. And Americans are inevitably going to read some of it, particularly if it's consistent with what they already believe.

So I gather what you're saying, Ms. DiResta, is the public has got to be alert to a repeat of the 2016 Russian playbook, which was to attract an audience on the left, discourage them from voting. And that could mean attacking Democratic candidates, pushing the line, in effect so that the Russians are trying to make it possible that our votes don't matter. Is that essentially your concern?

Ms. DIRESTA. Yes, sir. There's a lot of efforts to push intraparty divisions on the left.

Senator WYDEN. Good.

Let me ask you now, if I could, maybe for you, Ms. DiResta, Ms. Rosenberger, Dr. Kelly, about this concept known as down ranking. My interest here is that for the social media companies there's just a mismatch of incentives. The social media companies, they want users and clicks and impressions, and inflammatory and often false content creates that. So even when the companies can't or haven't decided to identify a certain account as either foreign or nefarious, they can still downgrade the posts to limit their exposure. This is

an equal or worse problem with conspiracies and junk news as it is with foreign influence.

So my question here would be for the three of you: Do you think these down-ranking programs are effective? Are they the kind of thing that ought to be considered part of the kind of toolbox as we look to deal with this problem, Ms. DiResta and the rest of you?

Ms. DIRESTA. Sure. So I think that there's sort of three facets to the toolbox. There is remove, reduce, or inform. Inform means to add additional context to a post. This is Facebook's framework right now.

Reduce would be to do something like down-rank it, per the question earlier about is it possible to inject just a little bit of friction? This is where down-ranking could potentially be used as a tool, as attribution and authenticity and integrity are established, to reduce the reach of content.

And then remove is, of course, the more—the most extreme.

Senator WYDEN. Would any of you like to add anything? Yes?

Ms. ROSENBERGER. I'd just like to note that we talk about down-ranking, but we forget that up-ranking is also part of the process. These platforms are not——

Senator WYDEN. You're being way too logical.

Ms. ROSENBERGER. These platforms are not neutral pipes.

Senator WYDEN. Right.

Ms. ROSENBERGER. Information is not being served up without some kind of algorithm deciding, for most of the platforms, without an algorithm basically deciding what is served up at the top. So when we talk about down-ranking, we have to start from the premise that up-ranking is baked into the cake. And so then the question becomes: are these platforms actually somehow prioritizing bad, malicious information, right? That, as we know and as others mentioned in their testimony, gaming these algorithms, whether that's on trying to get certain content to trend or, frankly, getting certain content to rise to the top of Google searches, something that we know that Sputnik and RT——

Senator WYDEN. I'm over my time. I just want to be clear, as the author of Section 230, the days when these pipes are considered neutral are over. Because the whole point of 230 was to have a shield and a sword. And the sword hadn't been used and these pipes are not neutral.

Thank you, Mr. Chairman.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you, Mr. Chairman.

So much of the activity we're looking at on the charts and today is largely of the IRA. What percentage of Russian-linked activity would you anticipate that the IRA represents? Is this half of everything they try to do, 90 percent, 10 percent? Who would have a sense of what we're not looking at when we're looking at the IRA activity?

Dr. KELLY. We've looked at a number of different known disinformation campaigns and we think these are—the IRA folks are involved in a minority of them.

Senator BLUNT. In a minority of them. Do you think that would be the case here as well?

Dr. KELLY. I do. The only thing—the thing we don't know, though, is how much of the IRA this is.

Senator BLUNT. Ms. Rosenberger, do you want to comment on that?

Ms. ROSENBERGER. I would just only add that we know from Special Council Mueller's indictment actually of the GRU, there is one section of that that notes that GRU operatives utilize social media accounts and fake Web sites that they created in order to spread hacked information and other kinds of weaponized information.

So we certainly know that there are other actors. GRU is probably better at hiding their tracks than the IRA is, and so I think that just speaks to again how this is probably just one tip of the iceberg of what we're looking at.

Senator BLUNT. So, the early discussion clearly has moved from what the Russians were paying for, which appears to be a very small fraction of the impact they were having. Does anybody disagree with that? That is clearly—and this IRA activity may—is some fraction of the Russian activity in 2016, 2017 and into 2018. That would be—so I think the indictment, the Mueller indictment, said that there were probably at least 80 IRA employees involved and millions of dollars involved in that effort.

I don't know what—is that 5 millions of dollars or hundreds, hundred million dollars? What kind of—what amount of money do you think the Russians invested in this effort that was covered by the Mueller indictment? He uses the term "millions of dollars." That could mean a lot of different things. Any idea of the activity you've looked at, what kind of investment of money and how many people that may have been involved in this?

Dr. HOWARD. We've done that audit globally. We believe that half a billion dollars have been spent by the 40 governments that we've studied since 2010. In the Russian case, we think it's around $200 million U.S. over this extended period for the full set of organizations behind the various campaigns.

Senator BLUNT. Dr. Howard, on that topic, in the other countries you've looked at, who should we be looking at after Russia that are likely impacting our daily conversation in the country, in some ranked order? Who would be the top three or four countries that you would believe would be most actively out there doing what Russia is also doing?

Dr. HOWARD. Well, in our research we look at Turkey, China, Hungary and Iran.

Senator BLUNT. Dr. Kelly, have a thought on that?

Dr. KELLY. We believe there's a growing black market for people skilled in the—who have these dark arts, and they're employing them in their own countries and they're also starting to get hired to work in other countries. So, this is a critical challenge, because the Russians may have been the first to effectively do this, but they're not the only players; and you'll have a black market of players who are mobile and can be hired by any actor.

Senator BLUNT. Well, just to be sure I understand, doctor, the 40 countries, are these 40 countries you've looked at for outside activity or 40 countries that are participating in this kind of activity?

Dr. HOWARD. These are 40 countries that have organized disinformation campaigns in the sense of stable personnel with

telephones and family benefits. These are formal organizations that do this work.

Senator BLUNT. And how many countries do you think they, those 40 countries, would be trying to influence activity in?

Dr. HOWARD. Seven countries.

Senator BLUNT. Seven countries?

Dr. HOWARD. There's seven authoritarian regimes that have dedicated budgets for disinformation campaigns targeting voters in other countries.

Senator BLUNT. And how many other countries, again?

Dr. HOWARD. Our audit of government expenditures covers 40 in total. It's usually the United States, Canada, Australia, the U.K. that are the—Germany—that are the targets.

Senator BLUNT. That are the targets.

On Dr. Kelly's comment about determining the attribution, you know, we have—in our country, we are focused on defense. No administration has yet figured out what our offense should be, and I think one of those reasons is we have not figured out with certainty how we would determine where a cyber attack came from as opposed to even cyber misinformation, which is a different kind of cyber attack, but vulnerable infrastructure. What we're seeing here is a vulnerable social media infrastructure that may be every bit as critical infrastructure as any of the other infrastructure we're trying to protect.

Ms. Rosenberger, I'm going to let you have the last answer to my questions.

Ms. ROSENBERGER. Senator, I would just note on that, that Russia is playing to its asymmetric advantage. This is a low cost, high reward kind of tactic. We need to also evaluate: what are our own asymmetric advantages and sometimes that's not responding symmetrically or in the same domain.

So, for instance when it comes to Russia, I think this is why imposing costs in the financial space in particular—we know that Putin cares most about his power and his power rests on his money. And I think that looking at ways that we can dry up the sources of funding both for these activities as well as for the regimes that are using them is incredibly important. When it comes to China, things like reputational costs are very important.

So I think, this is why it's important that we put this conversation on the national security front in a broader strategic frame to identify our own asymmetric advantages so we can go on offense.

Senator BLUNT. Thank you, Chairman.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Ms. Rosenberger, I believe it was you who said, and I may be paraphrasing here, but we've moved from a failure of imagination, to a failure to act. Do you find it troubling that, despite the current risk, despite the quickly approaching 2018 midterms, that concrete responses like the Secure Elections Act, like the Honest Ads Act, have not been scheduled for a vote in the United States Senate?

Ms. ROSENBERGER. Yes, Senator. I do believe that, while this is a complex problem, there are some clear steps that we can take in particular on the defensive side, as well as on the deterrent side, that we need to be taking urgently.

Senator HEINRICH. I share that concern, because I think some of these things are sitting right in front of us and we just need to make it a priority.

For Ms. DiResta and Dr. Kelly: The Committee's analysis shows that the Internet Research Agency's campaign focused heavily on socially divisive issues, but fanning racial division in particular was the single most targeted category of effort. Are Russian information warfare operations using unresolved racial tensions here as a weapon to weaken the United States?

Ms. DIRESTA. Yes, I believe they are.

Dr. KELLY. Absolutely.

Senator HEINRICH. Do you see that ongoing exploitation of racial tensions as a direct threat to our national security and, for that matter, our cohesiveness as a country?

Dr. KELLY. You could think of this as a social cohesion attack to try and drive wedges into the American public where maybe a little wedge or a piece of history in our past is being exploited to make 21st century America look more like 1950s America than it ought to.

Ms. DIRESTA. I would agree.

Senator HEINRICH. So, we now know much more about the Russians' 2016 campaign than we did before we started this investigation, and we know it was far broader than we originally thought. We know that it's highly active today, as many of you have testified to, and we know that no single entity by itself—not the government, the social media companies, not civil society—can effectively stop foreign influence operations on social media.

But, Ms. Rosenberger, in your view have we as a Nation extracted the sort of price or penalty for this behavior that would defer—deter Vladimir Putin from acting in this way? Or has the Russian Federation simply gotten a pass so far in terms of the price that we have chosen and that this Administration has chosen to extract?

Ms. ROSENBERGER. So, I think it's evident by the fact that this kind of activity continues, that we have not yet effectively deterred it. One thing I would note is that in classic deterrence theory, deterrence relies on two prongs: one is credibility and one is capability.

And I think it's incredibly important, number one, that on the credibility front we have very clear, consistent messages from across the government, starting with our leadership and all the way down, that they're——

Senator HEINRICH. Including the White House?

Ms. ROSENBERGER. Including the White House—that this behavior will not be tolerated and that there will be consequences for it going forward, and articulating what those consequences will be. And I think that there is a role for Congress to play here in terms of teeing up triggers that would be automatic, and I know there is consideration of such measures and I welcome that. But I think that it also has to start—the credibility piece has to be very, very clear.

Vladimir Putin cannot see from one place that there is a potential for consequences, but then over here be getting a very different

mixed message. We have to have consistency; that has to be credibility coupled with the capability to act.

Senator HEINRICH. I could not agree more.

You mentioned financial cost as one of our asymmetric advantages. What would you foresee as a potential cost that we might extract for this kind of ongoing misbehavior?

Ms. ROSENBERGER. I think there's two different ways of looking at it. One is, of course, very targeted sanctions and other kinds of designations; the other is thinking more broadly about how our financial system, the Western financial system, frankly, is used for Putin and his cronies to hide the money that they have stolen, by the way, from the Russian people.

And just as we have vulnerabilities in our information domain, we have vulnerabilities in our financial system. I think steps like providing transparency around beneficial ownership, extending and legislating the geographic targeting orders that the Treasury Department has been using—there's a whole suite of steps that we outline in our report that I mentioned earlier, that I think——

Senator HEINRICH. I will read those in the report. I want to hit one last thing and then my time is up.

You all mentioned the broader ecosystem. Can you just confirm so that people understand, this isn't just a couple of platforms? This is music apps, this is video games, this is meme sharing. It's much broader than Twitter and Google.

Dr. KELLY. I would expect that they have people whose job it is to figure out how to exploit every small new platform that comes along.

Senator HEINRICH. Thank you all.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman. And I want to thank—thank you, Mr. Chairman, for calling this, what I think is a very important hearing.

And thank you all for all the information that you've shared. I've been listening and came up with a couple of conclusions. Tell me if I'm right. One is: there is a massive, sophisticated, persistent campaign on multiple fronts to misinform, divide and ultimately manipulate the American people. Is that accurate?

Dr. KELLY. Yes.

Senator KING. I wanted to hear "yes" because nods don't go in the record.

[Laughter.]

Dr. HOWARD. Yes.

Ms. ROSENBERGER. Yes.

Senator KING. Let the record show everybody nodded.

Dr. HOWARD. Yes, Senator.

Ms. ROSENBERGER. Yes.

Senator KING. I think that's incredibly important because in all of this whole Russia active measures thing, a lot of the space and energy has been going into campaigns and elections and collusion and those kinds of questions. This is an enormous part of what's going on, and it worries me that we've sort of lost sight of this.

The second thing I've learned from you is, number one, it's still happening; is that correct?

Dr. KELLY. Yes.

Ms. DIRESTA. Yes.

Senator KING. Absolutely, still happening?

Ms. ROSENBERGER. Yes.

Senator KING. It's way beyond elections.

Ms. ROSENBERGER. Yes.

Dr. HOWARD. Yes.

Senator KING. Secondly, it's more sophisticated than it was in 2016. They're learning to hide their tracks, not paid in rubles. I would have thought they would have figured that out before. But more sophisticated.

And then finally, it seems to me what you've been suggesting is we're asymmetrically vulnerable because of the First Amendment and democracy. We believe—our whole system is based on information. And we have this principle of opening access to information. Thomas Jefferson said, "We can tolerate error as long as truth is free to combat it." Thomas Jefferson never met Facebook, I might add.

But would you agree that we are particularly vulnerable because of the nature of our society?

Ms. ROSENBERGER. Yes.

Senator KING. Now, this one is for the record because I think it's a long answer. It seems to me there are three ways to combat this. And the first—and this is what I would hope you would supply for the record—technical solutions. Things that have been mentioned today that we could do, and that Facebook could do, or Google, or Reddit, or Twitter, whoever. Technical solutions: identifying bots, for example, those kind of things.

Please give us some specificity and things that you think we might be able to do without violating the First Amendment. I shudder when I hear the words "regulate the internet." I don't want to do that, but there may be things that we can do that could be helpful.

The second thing, it seems to me—and, Doctor Helmus, you mentioned this in your testimony—we need to do a better job of media literacy. I had a meeting just before, in the fall of 2016, with a group of people from Latvia, Lithuania and Estonia. And I said, "What do you do about this problem with the Russians' propaganda? And you can't unplug the internet, you can't unplug your TV."

They had a very interesting answer. They said: "The way it works over here is, everybody knows it's happening and therefore when something like this comes online, people say, 'oh, it's just the Russians again.'" We haven't gotten to that point.

Doctor Helmus, is that what you mean by "improve media literacy"?

Dr. HELMUS. Yes, precisely. To be able to recognize these instances when they appear, and to be able to process those in a way that can minimize the impact.

Senator KING. But that goes—it's deeper than just having a hearing. This has got to be—you know, our kids are growing up with these devices, but not necessarily being taught how they can be manipulated by their devices. I think there ought to be standardized courses in high school called "digital literacy," and increasing the public's awareness that they are being conned, or that at

least they're potentially being conned, and how to ask those kinds of questions.

Ms. Rosenberger.

Ms. ROSENBERGER. Senator, I think that that's right; it has to include online literacy as well as just your standard media literacy. But it also can't just be in the schools. One of the things we know from research is that, in fact, it may be that older populations who are not growing up with technology may, in some cases, be more vulnerable to manipulation by this kind of activity.

Senator KING. I would argue that's because they grew up with newspapers and they have this unspoken assumption about editors and fact checkers.

Ms. ROSENBERGER. I think that's probably right, sir.

Senator KING. And if you do your website in Times New Roman, people will give it some credibility.

Ms. ROSENBERGER. Especially if it's your friend sharing it, or somebody you believe to be your friend, someone——

Senator KING. And your friend may be sharing something which they got from somebody that they didn't know where it came from.

Ms. ROSENBERGER. Absolutely, absolutely.

Senator KING. A final point, and I think you've touched on this, is deterrence. Ultimately, we cannot rely exclusively on defense. The problem thus far, it seems to me, is that the Russians in this case and others see us as a cheap date. We are an easy target with no results. Nothing happens.

And I would—that would be something I hope you all again could take for the record because of a lack of time, to give us some thoughts about deterrence. And I think it's important. It doesn't have to be cyber. It could be deterrence in a number of areas, including sanctions, as we've discussed.

But it has to be—there has to be some price to be paid. Otherwise, as we now know, it's going to continue.

So give me some thoughts on deterrence for the record. I appreciate it.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Senator King.

Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

I want to thank all of you for coming today to help us. This is a critical topic, which I hope all Americans are watching.

We, as an open voting society need to be informed. A properly informed voter population is the key to a sound democracy. Unfortunately, Russia is trying to undermine that foundation.

A quick look back through American history shows that our allies and adversaries have changed over time. The Soviet Union, specifically Lenin and Stalin, openly criticized the capitalist West before World War II. During our mutual fight against Nazi Germany, President Roosevelt called Stalin "Uncle Joe" and the U.S. and USSR fought a mutual enemy. After the end of the war, we found ourselves in an adversarial relationship, known as the Cold War that lasted decades.

We saw a brief thaw in relations during the 1990s. But now Russia, specifically Vladimir Putin, and the U.S. seem to be adversaries again.

I would ask, I think Mr. Howard, in your written testimony you describe Russian computational propaganda aimed at everything that we've heard today, pulverizing voters, discrediting certain political candidates, discouraging citizens to vote.

So I would ask, which country—we know Russia—poses the greatest threat to our democracy using social media platforms? And which countries are making strides to do the same?

Dr. HOWARD. Thank you, Senator. I agree that Russia has been the most innovative in developing these kinds of techniques. Unfortunately, I think it's safe to say that dictators learn from each other. So as they see successful campaigns run in particular countries, they emulate. They sink their own resources into developing similar capacity. Some of these countries have re-tasked small military units to do entirely social media campaigning.

So as I mentioned earlier, there are now seven different countries that are—who are, most would agree——

Senator MANCHIN. Actively involved?

Dr. HOWARD [continuing]. Authoritarian regimes that are actively developing these kinds of——

Senator MANCHIN. Which ones do you think—which one has the greatest potential to do harm? Russia is unquestionably the absolute greatest violator.

Dr. HOWARD. I believe China has the next best capacity in this——

Senator MANCHIN. If they want to turn loose on us?

Dr. HOWARD. If they want to.

Senator MANCHIN. And you haven't seen that yet?

Dr. HOWARD. Not directly in the U.S. sphere.

Senator MANCHIN. I would ask this to any of you all. Is there any country that has been successful at deterring Russia or any other attackers from other countries?

Dr. KELLY. Not that I'm aware of.

Ms. ROSENBERGER. It's hard to know the counterfactual of what would have happened in different cases in some of these instances. There is some evidence that in the German and French elections, that deterrent messaging from the top, from the leadership there about the consequences for this kind of activity, may have reduced in some ways the kind of activity.

Senator MANCHIN. How about Macron's election in France? We saw that he fought back. As soon as they saw the attacks being made by Russia, they were actively involved.

Ms. ROSENBERGER. There are some interesting lessons that we may be able to learn from——

Senator MANCHIN. Dr. Kelly. I'm so sorry——

Ms. ROSENBERGER. No, please, absolutely.

Senator MANCHIN. Our time is very limited.

Dr. KELLY. No, I answered too quickly before. I think the Macron case is a perfect example of how being aware of it, that kind of situation awareness, as well as quick and decisive action to counter it in terms of public—you know, speech by the leadership—had an effect.

Senator MANCHIN. And let me just ask—I've got one final question here. I have a little bit of time here, but I wanted to see your all's opinion. In West Virginia, you know, people are having a hard

time deciding where to get the facts. And fake news seems to be the real news, depending on where they get it from, social media and sometimes on networks, if you will.

Can I ask each one of you all, where do you receive your news that you believe is factual? Where do you go to? Where could I help a West Virginian find some real news and not have to rely on trying to decipher themselves was it fake or not? Is it made up, real or not?

And I'll start Dr. Howard and go right down.

Dr. HOWARD. I go to PBS, BBC, and the Canadian Broadcasting Company.

Ms. ROSENBERGER. I'm old-fashioned and I tend to still like newspapers as my sort of major sources. I like having publishers involved and editors who are able to fact-check content.

Dr. KELLY. I'm a New Yorker, and I'll go with the Old Gray Lady.

Ms. DIRESTA. New York Times, Washington Post, Wall Street Journal.

Dr. HELMUS. Major newspapers.

Senator MANCHIN. Not one of you mentioned social media. Not one of you all mentioned what we're here talking about as where you get you news or where you trust your news to come from. I think that speaks volumes of what we're dealing with today.

I have no further questions after that. Thank you very much.

Chairman BURR. Thank you, Senator Manchin.

And I just might add to his comment about what happened in France. France also did some things that constitutionally we can't do. So let's recognize the fact that they had a very loud message and they had a very big stick that they used. And we might not get the same results, though that doesn't change for the loud voice.

Senator Rubio.

Senator RUBIO. Thank you.

No one mentioned TMZ. There is some good stuff on TMZ.

[Laughter.]

And I'm on as often as I can get on there.

Anyway, so I want to talk about the terminology that we use because I think it's one of the things that's really impeding the way forward, and get your insight on all of this. The first is, I've had people come up to me and say: Well, everybody spies on everyone. But this is not really about espionage, certainly not in the traditional sense. This is not—I mean there may be elements that involve espionage, you know hacking a computer, getting into a system network and stealing e-mails and the like. But this is not really an espionage situation.

The other term that's always thrown around is collusion. And there's ongoing efforts to answer all those questions. But this sort of thing doesn't really involve, or doesn't really require collusion. You don't need the cooperation of a political candidate or party to be able to do any of this.

In fact, many of the ads that were pulled down yesterday have nothing to do with a candidate or a party in the short term. And it isn't even quite clear what the psychology behind it is, other than to get us to fight against each other.

So if you can just put—if people would just put aside the whole espionage focus and put aside, you know, the collusion focus, and let that be dealt with the way it's being dealt with, we'd get left with the term "interference." And that's become such a generic term that it's almost become benign. You know, "interference" sounds like everything from the leadership of another country had a preference about who won the election, to actually like actively engaged in helping somebody get elected. And I would hope—and, maybe you disagree—I hope you agree, this is more than that.

This is really, no, nothing less than informational warfare. This is just another type of warfare to weaken an adversary. And that's how Vladimir Putin views the United States of America. So, for example, if he conducted a kinetic strike, a military strike to take out anti-air defenses, he would do so to weaken our air defenses. And if they conducted a cyber attack to knock out our command and control, he's there to weaken our communication systems or our electrical grid.

And if you do this, you do it in order to weaken our society, our willingness and capacity to fight, to work together, to come together as a Nation. This is part of their broader doctrine on how to confront an adversary.

And on the escalation scale, it costs very little money, you can do it with limited attribution, and it works because the fact of the matter is, with all of the things happening in the world today, the United States Senate Select Committee on Intelligence has spent an inordinate amount of time on this important topic and there are so many other issues we could be focused on. So, it's worked to some extent.

Is this assessment of it right? Isn't this—this is not interference. This is information warfare designed to sow division and conflict and doubts about—because whether it involves changing voter registration databases in the future at some point, potentially, or the stuff we're seeing now, all of that is designed to sow chaos, instability, and, basically, to get us to fight against each other.

We're already fighting against each other in this country. All this does is just, sort of, stir that up even more. Is that an accurate assessment? Is this informational warfare?

Ms. ROSENBERGER. Yes.

Dr. KELLY. I agree 100 percent.

Ms. DIRESTA. Yes.

Dr. HOWARD. Yes.

Senator RUBIO. So to the extent that it is—and I think everybody's already asked you this question—but wouldn't one of the best things that could happen is that—we can focus all day on Facebook and Twitter, and Instagram. These are ultimately platforms who are being used for informational warfare. I don't believe they invited them in and there are things they can do to improve their processes, and I wish their disclosures were a little faster, but by and large, they're a platform that's being used. It would be like blaming the road builders because some enemy used that road that they built to put their tanks into your country.

So there are things these folks can be doing to improve the way they operate, no doubt about it. But ultimately, we really should

be focused on what's being done and not only who they're using to do it.

And so my question is, why wouldn't these social media pages be in a position to potentially alert all of their users? Not just a public disclosure like they did yesterday in their press conference but actively send out to all of its user's alerts about every time they remove something, so that people can become conditioned to the sort of messages that are being driven by these informational warfare operations?

Ms. DIRESTA. I believe they can. I believe Senator Blumenthal requested that they do so in response to the—back in September after the first set of hearings. They did push notifications to people saying that they had seen content, they had liked a page, they had engaged. I believe Twitter sent out e-mails to users who were affected.

That kind of disclosure is absolutely necessary, because one thing that it does is it comes from a platform that is at least seen as somewhat trustworthy, whereas if they hear it from the media you see these polarized echo chambers where some people don't even believe this is happening.

Ms. ROSENBERGER. Senator, I would just add that one of the things we know from looking at both the history of active measures as well as their use across Eastern Europe and Central Europe is that sunlight is one of the most effective antidotes. Transparency, exposure of this activity, is critical for both building resiliency and deterring it going forward. And so, I absolutely concur that the more information and the more transparency that the platforms can be providing to their consumers, to the users of information about these activities is absolutely critical.

Senator RUBIO. I don't have a question, Mr. Chairman. I just want to say that it's great that Facebook put this stuff out there and that we're having this hearing. I promise you, the vast majority of people that I know back home will never see a single one of these images because there's a lot going on in the news every day, constantly, by the hour.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

Mr. Chairman, I'd like to put what I believe is a context in which we should be thinking about what happened in 2016. First, I think we're all clear that Russia attacked our country during the 2016 election and that they are continuing to attack us today. Russia not only attacked one of our most sacred democratic values, which is a free and fair election, but also I believe our very American identity.

I often say that we, as Americans, no matter our race, religion, or region, have so much more in common than what separates us. And among what we have in common is a love of country and a belief that we as Americans should solely be responsible for the choosing of our elected leaders and the fate of our democracy and who will be the President of the United States.

And I think of us then as being a large and diverse family, the American family. And like any family, we have issues and fissures that are legitimate and run deep and provoke potent reactions. We have a history of slavery in this country. We have a history of Jim

Crow, of lynchings, of segregation, and discrimination. And, indeed, we have a lot to do to repair and to recover from the harm of the past and some harm that continues today.

But let's be clear. Someone else came into our house, into the house of this country, the family of who we are as Americans, and they manipulated us; and they are an adversary, and they provoked us and they tried to turn us against each other. The Russian government came into the house of the American family and manipulated us.

And we must take this seriously in that context and understand that when we debate, as we did in 2016, one of the most important debates that we have, which is who will be leader of our country, the Russians exploited our Nation's discourse to play into our deepest fear.

And as leaders I believe then it is incumbent on us to speak to the American people about how we can solve this urgent national security threat. I believe, first, we must act urgently to bolster our country's defenses like our election infrastructure and cybersecurity, a bipartisan issue that we have been working on in a bipartisan way—I thank Senator Lankford and many of our colleagues—throughout the work that we've been doing on the Secure Elections Act.

But second, I believe we need to make sure that the American public recognizes who is trying to sow hate and division among us, so that the American public can rightly identify and see it for what it is: an attempt to exploit our vulnerabilities for the purpose of weakening our country and our democracy.

And with that, I'd like to ask, Ms. DiResta, in your written testimony you say that the Russian Internet Research Agency, IRA, efforts targeting the right-leaning, quote, "right-leaning and left-leaning Americans was unified in its negativity towards the candidacy of Secretary Clinton"; and that, quote, "in pages targeting the left, this included content intended to depress voter turnout among black voters."

This seems to corroborate the intelligence community's finding that Russia was trying to hurt the campaign of one candidate in the 2016 United States election and help the other. Can you tell us more about what your research has found regarding the nature of the political content that the Russian IRA was pushing toward Americans on social media during the 2016 campaign?

Ms. DIRESTA. It was unified on both sides in negativity toward Secretary Clinton. It was not unified in being pro-President Trump. So the pages targeting the left were still anti-candidate at the time Trump.

On the right, we did see an evolution in which evidence of support for candidate Trump continued during the primaries. There was some anti-Senator Rubio, anti-Senator Cruz content that appeared. And there was a substantial amount of anti-Secretary Clinton content on both the right and the left.

On the left, that included narratives that either African Americans should not vote, should vote for Jill Stein, which was not a wasted vote, and during the primary there was support for candidate Sanders.

Senator HARRIS. And then quickly, Ms. Rosenberger, you recently published a report policy blueprint for countering authoritarian interference in democracies. You described an event on May 21 of 2016 where two groups were protesting in Houston, Texas, and one was called the Heart of Texas that opposed the purported Islamification of Texas. On the other side, the United Muslims of America, who were rallying to purportedly save Islamic knowledge, and these protests were confrontational.

Can you tell me, at the time were law enforcement or the protesters aware of who had manufactured the conflict?

Ms. ROSENBERGER. No, our understanding is that they were not. One thing we do know is that, fortunately, law enforcement was present at the demonstrations and therefore was able to keep them separate. But one of the things that we believe may have been part of the intent of organizing simultaneous rallies—same day, same place, opposite sides of the street—was probably to attempt to provoke violence.

Senator HARRIS. And then just quickly, if we can follow up in any writing with the Committee, but I'd be interested in knowing what your recommendations are for how we can inform law enforcement, because obviously this is a matter that is about public safety and frankly also officer safety. As we know, many of these disruptions end up resulting in violence and harm to many individuals.

Ms. ROSENBERGER. Absolutely. I would just point very quickly to the announcement from Facebook yesterday, which actually seems like it may have been something intended to be along similar lines with a protest attempting to gin up very high emotions.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you, Mr. Chairman.

To all of you, in your research and the data that you're putting together to be able to help us in this and be able to expose some of the issues, thank you. You all have done a lot of hours at a computer and running a lot of data to be able to get to this point. And we appreciate that very much.

Ms. Rosenberger, I want to ask you about some of the recommendations that your team has made and to follow up on one of the questions that Senator Blunt had started. You made some very specific recommendations that, when we discover attribution, which is not easy to do, but when we discover it and see it as a foreign actor, three main sets of responses you seem to have recommended: sanctions; making sure there's a reputational cost for the country that's doing it; and considering offensive cyber operations. I want to take those in reverse order.

What would you consider an offensive cyber operation that would be effective in this means?

Ms. ROSENBERGER. Well, Senator, as you know, the use of offensive cyber operations is itself a very complex problem.

Senator LANKFORD. Right.

Ms. ROSENBERGER. So I'm just going to kind of boil it down to be specific within this context.

What I would say is, I think that there are instances in which when we are able to—when the U.S. government is able to identify— for instance, the servers that are being used to carry out these operations, based on a variety of potential damage assess-

ments, et cetera, I do think that there are instances in which that might be an appropriate course of action.

Again, as we know in offensive cyber, this can often lead to a challenge of whack-a-mole. You set up a new server, et cetera. It does impose a cost. Of course, one of the things that we know that creates challenges is sometimes for these transnational operations they may, for instance, be using a server in the United States, or in the country—or in the domain of one of our allies. So that introduces complications.

So it's not a super-simplistic answer. But I do think that there are instances in which we should consider it.

Senator LANKFORD. So you also mentioned reputational costs. I'm not sure there's anyone left on the planet that doesn't understand that Russia does propaganda on their own people and does offensive propaganda against everyone else.

What kind of reputational cost could you put on Russia, trying to expose their activities?

Ms. ROSENBERGER. Senator, the reputational cost recommendation is a little bit more specifically aimed at China, where I think that, as others have alluded to, China has the capabilities and we're seeing them test these things in their neighborhood. China has a longer-term strategic interest that's much more about generating affinity toward it and its model. So I think that reputational costs would be more effective with China.

I concur with you that, when it comes to Russia, reputational costs are difficult, although I do believe that it is important for the American people to hear clear and consistent messages from our leadership that Russia and Vladimir Putin are an adversary and a threat to our Nation.

Senator LANKFORD. It was one of the areas that I was pleased with Facebook's announcement yesterday that this Committee had talked to Facebook about multiple times. It's one thing to be able to say that they are being used by an adversary; it's another thing to actually show the images.

Ms. ROSENBERGER. Yes.

Senator LANKFORD. Yesterday Facebook was rapid to not only say there's an outside entity, we're not saying it's Russia, it looks like it is, but here's the images they're putting out, here are the events they're putting out. And they put out a tremendous amount of data yesterday. That's much improved from where we were two years ago, where they were still saying, "We're not sure if they used us or didn't use us." Now they're being very forward-facing on that. That's helpful to be able to get information around faster.

Traditional media multiplied that message by putting it out as well. That helps us to be able to get the message out. That's one of the things that we heard on this Committee multiple times: European allies have faced from Russia those attacks, that they've been able to get that and have that pushback immediately. So that was helpful to be able to see it yesterday.

I have one other question to relate to this as well. You had mentioned a comment here in one of your recommendations on making sure that there is transparency, passing legislation that ensures Americans know the source of online political ads. Much of what

happened with this was not an ad. It was just a profile that was set up that they did a tremendous amount to be able to develop it.

How do you separate out being aware where an ad is coming from and just a profile that's a free profile, that's developed quite a following?

Ms. ROSENBERGER. I completely concur that the political advertising piece of this effort was a small one. My own view, coming from a national security perspective, is when we identify a vulnerability we should close it off. And so even if it was not the most significant avenue that was utilized, I absolutely believe that applying the same standards to political advertising online that apply offline is absolutely essential. That being said, that will not solve the problem and we can't be in any way convinced that it will.

And so that's why we also recommend a number of transparency measures about providing greater context for users, about the origin of information, about whether automation is involved, about requiring some kind of authenticity confirmation while protecting anonymity. I think these are the kinds of steps that can help mitigate some of these broader concerns that you're raising.

Senator LANKFORD. I look forward to that conversation. We also need to have a conversation on is there a level of cooperation needed between the internet service providers, cell phone companies, and others that have a different level of information about where that information is coming from, and their cooperation with some of the providers of content.

Right now we're leaning mostly on providers of content to say, help us with the data and help police yourself on it. But there's another whole level of information coming from the ISPs and from the cell phone companies and such, as well, of where that data is actually originating from.

Ms. ROSENBERGER. Absolutely. And when you combine that with information that the intelligence community can provide, I think that that is how we begin to put together different pieces of this puzzle to create better identification processes.

Senator LANKFORD. I look forward to that.

Thank you, Mr. Chairman.

Chairman BURR. Senator Reed.

Senator REED. Well, thank you very much, Mr. Chairman, and thank you all for your excellent testimony.

We all here appreciate what Facebook did yesterday. I think it was a very appropriate and timely response. But there was a comment that you made, Dr. Howard, that I think is very important and bears repeating, which is basically that companies are beyond self-regulation. Could you elaborate on that, and then I'll ask the panel if they concur?

Dr. HOWARD. I think much of what we've discussed today has come from evidence that has been released very slowly over a two-year period, often after prodding from you, multiple kinds of Committee investigations and multiple governments. When I say that I think the social media industry is past the point of self-regulation, I mean mostly that the more public, open data there is about public life, the faster we can catch these moments of manipulation.

For the most part, we've been speaking about American citizens and us as individuals and the impact on our—on our democracy,

but democracies have civil society groups, faith-based charities, civic groups, prominent hospitals and universities that are also under attack. And these are also distinct to democracy and these are part of—these are the organizations that I think can help defend us.

Senator REED. But I think, again, we have and we have gotten—and Chairman and the Vice Chairman have done a remarkable job. We've gotten, as you say, slowly and surely we've gotten a little bit more response. But I think the time is running out, frankly, and I think we have to move legislatively to set in motion a framework of disclosure.

Someone mentioned, you know, options to remove information, reduce information, or inform the participant. I don't think that will happen voluntarily. It's the prisoner's dilemma. I'm sure they would all love to do it, but unless everyone does it it's not cost-effective or it's not culturally consistent with their corporation.

So, let me just go with Ms. Rosenberger and down the line about this comment about do we have to move very quickly to set up the framework, consistent with the First Amendment obviously, that allows us to deal with this issue?

Ms. ROSENBERGER. Senator, one thing I would note is that, while the United States has not taken any steps like this, other countries or international institutions have. So the European Union has been moving out, not just with GDPR but other conversations about regulation of social media and online platforms. China is using its market access as enormous leverage over these companies in order to basically set the terms of the debates.

By being absent from this conversation and not taking steps to figure out some of these very thorny issues, but right now what's happening is other countries, other governments, are setting the rules for this space. And that is in many cases not in the interest of the United States. I think some of the ideas that Senator Warner put forward in his paper earlier this week are absolutely worth very, very serious conversations and the kind of things we need to be doing.

Senator REED. I think one of the ironies, as you point out, is that we could be disadvantaged because not only don't we get to make the rules, but our companies, our international companies, will follow the rules in China, follow the rules in Europe, and not follow the rules here, leaving us much more vulnerable.

Dr. Kelly.

Dr. KELLY. I believe that it's critical to have access to data from all the platforms in order to detect this kind of activity. And that is a sophisticated analytic capability that needs to be created, and it's going to be a lot of time and effort from a lot of smart people.

Where does that data then sit? Who is it that gets to look at it? And I think that our concerns about privacy and the First Amendment lead us to at least suggest we ought to think about industry-oriented consortiums or things that allow a kind of—without moving it too far from industry—let them at least have the first crack at the detection piece.

Senator REED. Well again, I think your instincts are very consistent with the views of most Americans. But this now has been several years, and we are still waiting for the kind of robust re-

sponse. Perhaps the Facebook example yesterday is a good sort of sign that the industry is coming around, but——

Dr. KELLY. Yes, Senator. I think that the proactive transparency we saw yesterday from Facebook shows real leadership in the field. And I think we need more of that.

Senator REED. We do, and my concern is that, again, there are other incentives, disincentives, profit, culture, et cetera, that could inhibit that.

My time is expired, but ma'am, please.

Ms. DIRESTA. I think the key is to have oversight. We spoke about finance a little bit earlier, high frequency trading in particular. There were two sets of regulators. There were self-regulatory bodies that stepped in, there were the exchanges. There're some parallels there, where the exchanges are able to see what's happening and immediately, before the regulatory process happens, step in and say: Not on our platform.

I think that that's actually an interesting model; this combination of regulatory, self-regulatory, the exchanges acting independently, and an oversight body looking to make sure the entire ecosystem remains healthy.

Senator REED. You're talking about the security exchanges?

Ms. DIRESTA. Correct.

Senator REED. Yes.

Doctor, comment?

Dr. HELMUS. I'll just say our research certainly shows the importance of tagging this information so that audiences can know the source of it. The appropriate legislative mechanism for that I can't speak to.

Senator REED. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Cornyn.

Senator CORNYN. I can't help but recall the words of H.L. Mencken, who said that for every complex problem, there's a solution that is clear, simple, and wrong. And so I think we need to be a little bit—demonstrate a little humility when we begin to approach this from a public policy perspective, what our response should be.

But I also want to ask you about my impression, which is, it would be a mistake to think this is just about elections. And one of the reasons I say that, I came across an article recently entitled "When A Stranger Decides To Destroy Your Life," where somebody used a fabricated story about a woman and posted it online on a website called "She's A Homewrecker," and basically ruined this woman's life, or at least challenged it in a dramatic way.

And then I thought, well, this is a tool that could also be used by somebody who wants to tank a stock price by disparaging the reputation of a company and then perhaps sell it short and reap a significant reward. Or, if you're a Chinese telecom that wants to get rid of some of the competition, particularly when it comes to developing 5G technology or some other cutting edge technology, this is also a pretty useful tool, using this information warfare.

So all of this leads me to wonder if by focusing solely on the election, which is dramatic and of tremendous concern—and I share the concerns of all of you and all the Committee—that if we just

focus on that and not the rest of the picture, whether we are missing the right picture.

Ms. DiResta, do you have any observations?

Ms. DIRESTA. Yes sir. We look at—at New Knowledge, we do look at misinformation and disinformation targeting corporates. On the state actor front, we have seen evidence of campaigns targeting agriculture and energy as two industries of interest to foreign powers. On energy, we've seen anti-fracking narratives, anti-fracking bots, by countries affiliated—countries with strong oil interests. In agriculture, that's taken the form of spreading fear about GMO's.

Senator CORNYN. Yes, Ms. Rosenberger.

Ms. ROSENBERGER. I'd also note that in the case of Russia, we know that they use these operations to try to shape our conversations and views on geopolitical issues, especially those of interest to Russia.

So for instance, one IRA-sponsored post on the fake—the inauthentic account "Blacktivist" asked, how would we feel if another country bombed us for the poisoned water in Flint and for police brutality? That was posted in the immediate aftermath of the Trump Administration's strikes on Syria after the chemical attack in March of 2017. So a clear instance of that account actually criticizing an action by the Trump administration, using emotional issues like the Flint water crisis and police brutality as an avenue in, to try to shape views on a geopolitical issue of interest to Russia.

Senator CORNYN. Dr. Kelly.

Dr. KELLY. So I completely agree that there's a commercial dimension of this which is underreported, and there's a lot more going on in the commercial space in terms of these attacks than is reported. Renee discussed some of them.

We've seen others with our customers. And sometimes they're tied, these political attacks and the attacks on corporations, where corporations will be basically punished with falsely amplified boycott campaigns and similar measures for doing something which is politically not what Russia would like to see.

Senator CORNYN. Dr. Helmus, the psychologist Jonathan Haidt gave a speech I saw online recently called "The Age of Outrage" at the Manhattan Institute, where he basically describes a narrative where there's a lot of things conspiring to manipulate us and invoke outrage for whatever is going on, whether it's cable news, social media or the like.

What can regular Americans do to protect themselves against those, whether they be state actors, whether they be individuals, whether with malicious intent? What can they do to protect themselves? There's one thing for the government to do what we can do from a policy standpoint, but what can average individuals, consumers of social media online, do to protect themselves from being manipulated by fake information or misinformation?

Dr. HELMUS. You know, our work, our work in Eastern Europe, as was mentioned earlier, suggests that people in those areas are very well aware of Russia's intentions. Russia lurks very closely to those nations, and people know what's going on.

I think obviously the way to apply that to the United States is understanding the need to know the sources of your information,

be able to adjudicate and assess the truthfulness of that information, the potential biases of that information, and then try to make your own decisions on that. Ultimately, it's about being a careful consumer of information.

Senator CORNYN. Thank you.

Chairman BURR. Thank you, Senator Cornyn.

The Chair's going to recognize himself for just a question, and then I'm going to recognize the Vice Chairman. We'll see if we've got any members that return after that second vote starts. But it's my intention to try to wrap up as close to noon as we can.

You know, I've heard a lot of phrases to describe what went on just in the last few minutes—disinformation campaign, misinformation campaign, societal chaos campaign. Dr. Howard, I think you used one that struck me earlier—computational propaganda. And my suggestion is that we not come up with a single one, because we're dealing with a generational issue. And I think somebody alluded to it earlier, that it's much easier to take a generation that grew up with these devices and accomplished some type of change than it is for somebody that struggled, like me, to learn how to use the device and found the most useful TV ad, when somebody defriended somebody they took their picture off the wall, if you remember that Post-It note? That struck home to me.

So I think it's important that we speak to as many languages on this, because the task that we've gotten before us is to penetrate the entire population. And it's not limited to the United States. As you have described today—and, you know, I hope if there's a takeaway for the media—this is going on everywhere. It's not limited to politics. It's much more intrusive in the economic, global economic picture today, than it is in the political landscape.

It's just we like to write about politics. And so, I want to point you to this chart I've got over here. It looks like something that would be used at the psychiatrist's office, to have you describe what it was. And I'm going to ask you, Dr. Kelly. In our analysis, we went through and we tried to connect the dots: Who generates it, where does it go, does it go to the right, does it go to the left? And what my staff determined—and I'm looking for your agreement or disagreement—is that in a lot of cases, at least in the '16 cycle, the same person sitting somewhere in the world generating, initiating this propaganda, both initiated the part on the right and the part on the left, that it wasn't two different individuals. Therefore, this was a very well-orchestrated, very choreographed plan that they carried out.

What's your comment on that?

Dr. KELLY. Well, this is very interesting and it tells a deeper part of the story that the Clemson—recent Clemson paper tells, which is that you don't just have, you know, one room full of people who are running right-wing trolls and another room full of people running left-wing trolls. It's actually the same people at the same computers. So, I think that is a real lesson in how we need to worry about the way they're trying to play us like marionettes, right and left.

Chairman BURR. And is it safe to say that it's so easy that Russia uses existing views inside of American society; all they do is try to make the gap bigger between the two by inflaming both sides?

Dr. KELLY. I agree. I think that they're not creating these divisions. They're not—you know, and they're doing the same thing in Europe and elsewhere. They find in a society what are the vulnerabilities, what are the groups that oppose each other, and they're basically arming them. It's kind of like arming two sides in a civil war so you can kind of get them to fight themselves before you go and have to worry about them.

Chairman BURR. So, Ms. Rosenberger, is this any different than really what we faced in the 1960s in the campaigns by the Soviet Union against their adversaries in the world of propaganda?

Ms. ROSENBERGER. It is and it isn't. I think the playbook in some way is the same, but the tools that they can use to run those plays are very different. And what we have seen is that digital platforms have supercharged the ability to take that playbook and to really reach a much broader audience more quickly and in a much more targeted kind of way than what we would have seen in the 1960s.

There's a difference between hand-cranking out leaflets in a basement and passing them around under covert means than there is from putting information online using automated techniques, inauthentic personas, to watch it go viral.

Chairman BURR. I will say that the Vice Chairman has been one of the most outspoken about how technology allows this plan to be on steroids. Words like bots, and he comes up with some new ones every day, that many on the Committee and most in the country either didn't understand at the beginning of this or still don't understand.

So I'm not sure that we can emphasize enough the intent, but, more importantly, the capability, and he deserves a tremendous amount of credit for raising this to the level that it is.

I recognize the Vice Chair.

Vice Chairman WARNER. Thank you, Mr. Chairman. That's the nicest thing you've said about me and you said it with no members here.

[Laughter.]

Chairman BURR. I can repair the record.

Vice Chairman WARNER. You can repair it.

Well, I want to start with what Senator Cornyn and you just said. I think the political piece of this is really going to be relatively small compared to the overall threat. And I think one of the things we've not talked about yet today is the marrying of cyber attacks with misinformation and disinformation.

So, if somebody goes out, and let's say, for example that the Equifax hack was actually done by a foreign actor, and it's got personal information on 146 million Americans, then that actor contacts you with your personal financial information, you're going to open that, open that message. And then, if behind that messages comes a live-stream video of what appears to be Mark Zuckerberg or Jay Powell, the Chairman of the Federal Reserve, the ability to wreak havoc in the markets, it really almost overwhelms what we've seen on the political front. So this cyber-misinformation combination is one that's important.

I appreciate when we were talking earlier and recognize the rest of you—you really helped me recently—that even something that seems so obvious as should we have the right to know whether

we're being contacted by a human being or a bot has layers of complexity to it. But I think we ought to continue to explore that.

Ms. Rosenberger, I've got two points I want to make. One is: you have rightfully said we want to make sure that we protect anonymity, particularly, you know, the foreign journalists in Egypt or the female journalists in Egypt, and the ability to hide sourcing gets easier and easier with the use of virtual private networks.

Even with those challenges, shouldn't we have some ability, though, to say if—should an American have some ability to put some kind of geocoding location so that if somebody says they're posting a message from Michigan or North Carolina and it's originating in Macedonia or Russia, you ought to at least have that information? Again, you can still—we don't have to get to content, but we can just know that there ought to be a second look, because the origin of that post may not be what is described in the post.

Is that a possible tool?

Ms. ROSENBERGER. I think that there are ways that can be—that's one thing can be investigated. I think there are a variety of ways to require authenticity without requiring disclosure, sort of frontally, right? So a platform—in fact, some of them actually do require confirmation of authenticity.

Some of them require—some of them include a verified check that then sort of puts another label of—another level of sort of authenticity on top of that.

But I think that there are ways that authenticity can be confirmed or at least we can do a lot better to try to confirm it, while still ensuring that we do have anonymity protected and—sorry.

Vice Chairman WARNER. Let me follow up on that, because we've heard today some members talk about Section 230. We've heard some members talk about GPDR and the whole privacy bucket. You know, I've raised some issues about humans versus bots. We're talking here about geocoding.

One of the areas that we haven't talked so much about—and I'll appreciate the Chairman giving me this extra time—but are there market forces that could help regulate if we ensured more competition? For example, I was an old telecom guy and it used to be really hard to move from one telco to another until we implemented requirements of number portability.

You know, the Facebooks, the Googles, the Twitters dominate the markets. There may be, as people increasingly have concerns about the safety of their data, the ownership of their data, fake accounts being used—and this doesn't completely work as an analogy; let me state that up front. But the notion of data portability, the notion that would say: if you want to take all of your content off of Facebook, including your cat videos, they have to make it in a user-friendly form to move to NewCo, because NewCo as part of their business model is going to have much higher levels of authentication.

I mean, is this—is that a possible avenue to look at, as well? And I'll take anybody on the panel. Now, and when you get into data portability, you've also got to get into interoperability issues, which makes it again not a perfect analogy. But is there a nub of an idea there? Anybody?

Dr. KELLY. I don't have an answer on that exactly, but I think as you're thinking about that it's important to think that, in these kinds of disinformation campaigns, two of the most powerful things are a combination of anonymity and atomization. You know, those two things together allow you to run very large bot armies, so to speak, that are able to effect your objectives. It's important—so those two pieces are something you have to think about, how that concern weaves through this.

The other thing to realize, though, about that is that the bots are only part of the army, so to speak. So by solving that problem, even if you force them to identify, you've basically forced a medieval army to, you know, put a flashing light on the archers. There's a lot of other folks out there that are playing more direct roles that you still have to worry about. And I think that those more high-value assets in this kind of cyber social battle are a little bit harder to find. And they're the ones that, you know, you can't just fire up another—another hundred of them if you shut—if you shut the first one——

Vice Chairman WARNER. We've done a lot of recognition of Facebook today. I think we should also recognize Twitter, which in the last two months has, you know, even counter to their business model, has taken down lots of fake accounts, lots of fake bots.

But is there any, you know—is there any possibility here about trying to add more competition into the marketplace as a way to help us sort through this? Not so much just a regulatory approach, but a competitive approach?

Ms. DIRESTA. I'd say one of the challenges is if you fragment the platforms and fragment where people are, then there are more platforms to watch, since this is a systems problem and it does touch everything. That's not to say that that's not an appropriate course of action, because one of the reasons why this is so effective is there is this mass consolidation of audiences as the internet, which was originally much more decentralized, kind of came to have mass standing audiences on a very small handful of platforms.

The challenge there is also, though, that people like that consolidation. They like having a lot of—you know, all of their friends on one platform. So this is a—it's kind of a chicken-egg problem to think about it in those terms, but happy to continue the conversation.

Vice Chairman WARNER. I would just—if anybody wants to add, my last comment would be: I think one of the earlier statements that were made was that each of these platforms, even as large as they are, really only look after their own content or their own usages. So that ability to see across the whole ecosystem is mostly lacking.

And I think the Chairman and I—and we spent a lot of time trying to learn up on this—feel like the U.S. government is trying to get a handle on this, but has got a lot of work to do, as well.

So I really want to thank all of you. And one of the things that we might be able to find consensus on, you know, is there more ability for us to urge, force, nudge the platforms in an anonymous way to share more data with independent researchers? Because

you guys actually can give us that system-wide view that, for all the size Facebook has, Facebook can't give us the complete picture.

Ms. ROSENBERGER. Senator, I think that that's exactly right. I think we need two different kinds of information sharing, and ideally, they can somehow be combined. One is greater data-sharing between the public sector and the private sector, bringing together the capabilities of the U.S. government and the intelligence community, with the capabilities and what the platforms are able to see happening in their own ecosystem. Of course, that needs to be with privacy and speech protected, but I think there are mechanisms to do that, number one.

Number two is cross-platform information sharing. So I would think about this as both a vertical and a horizontal challenge. And then you have the question of outside researchers, which is absolutely critical. I think that Renee mentioned earlier the Global Internet Forum to Counter Terrorism. I think that's one model to look at in this space.

There's other models, including from the financial integrity world as well as from the cyber security world, where you have been able to bring together different parts of industry, academics and the government to ensure that the full picture is put together to best go at this problem.

Vice Chairman WARNER. Well I just want to again thank all of you, but I also particularly want to thank the Chairman, his notional idea. He did get this beyond taking the Post-It note off the refrigerator. But he has been a great ally, has moved this Committee forward on a whole host of technology issues.

This is one where there is no Democratic or Republican answer, since clearly the goal of our adversaries was not to favor one party over the other. It was to wreak havoc and split divisions. And I think this Committee, under your leadership, is trying to take this issue on in an appropriate way.

Thank you, Mr. Chairman.

Chairman BURR. And I thank the Vice Chairman.

You know, I was just sitting here thinking a lot of good has happened since we started this drumbeat over a year ago. A lot of changes have happened that I think 12 months ago at some of the companies we would have said "Never do."

A big ship is not turned around overnight. It takes a while. But I think that they have now given us an opportunity to work with them. And I hope that in a month, when we have at least three of the platforms in, that we will see a willingness to collaborate with us, to come up with a solution that fits both legislatively and from a standpoint of their corporate responsibilities.

So I'm optimistic that we're headed—that we're started on that pathway to a solution. You know, I remind people that it was this Committee that took on legislation for cyber security when everybody said it couldn't happen. Is it perfect? No. Was it a good first step? Yes.

And part of the challenge, because we're the filter for technologies changes in the world—there's no Committee of Technology in Congress, there's no Agency of Technology in Washington. It all sort of dumps in our lap, and we have a perspective that nobody else has. And technology will drive, for the next 10 years, the way

we do things, the way we communicate, where we go, how we do it. Everything in life is going to be driven by technological change.

So, this is very appropriate that we would be talking about a new architecture, not necessarily a new architecture for social media, but a new architecture for the relationship between government and the private sector.

And I hope that if there's a takeaway from today's hearing, it's that this is the last time we're going to associate the propaganda effort that we see, with an election cycle. There's been no interruption since 2016. There was no interruption from 2014. This was planned out well before we knew who two candidates were, we knew the differences between two parties, or where the American people's hot button was. It's flexible enough and it's nimble enough that it's going to attack whatever the hot button is at a given time that they want to initiate.

I can't thank all of you enough for your candid and insightful testimony. You've given us a lot to think about as we wrestle with how to counteract the problems of foreign influence and its use on social media.

I want to summarize what we've heard today for the American people. The Russians conducted a structured influence campaign using U.S.-based social media platforms and others to target the American people, using divisive issues such as race, immigration and sexual orientation. That campaign is still active today. They didn't do it because they have political leanings to the right or to the left, but because they—or because they care about our elections—but rather because a weak America is good for Russia.

Some feel that we as a society are sitting in a burning room, calmly drinking a cup of coffee, telling ourselves this is fine. That's not fine, and that's not the case.

We should no longer be talking about if the Russians attempted to interfere with American society. They've been doing it since the days of the Soviet Union and they're still doing it today. The pertinent question now is: what are we going to do about it? And it won't be an easy answer. The problem requires all of us—government, private sector, civil society, the public—to come together and leverage our distinct strengths and resources to develop a multipronged strategy to counteract foreign attacks.

We've heard about the problem today and have considered some potential recommendations and solutions. The next step is to hear from the leaders of social media companies themselves. And I'm certain that they, too, learned a fair amount today while watching this hearing, and I look forward to their responses. They owe it to the American people to communicate clearly and transparently what they view their role to be, and what they're doing to combat these foreign influence operations.

As I mentioned previously, this issue goes far beyond elections. We're fighting for the integrity of our society. And we need to enlist every person we can.

With that, I want to thank you for your time today. I think I've hit within about a minute of what I told you our target would be. This hearing is adjourned.

[Whereupon, at 11:58 a.m., the hearing was adjourned.]

Supplemental Material

Russian Social Media Influence

Understanding Russian Propaganda in Eastern Europe

Addendum

Todd C. Helmus

CT-496/1

Document submitted August 30, 2018, as an addendum to testimony before the Senate Select Committee on Intelligence on August 1, 2018.

For more information on this publication, visit www.rand.org/pubs/testimonies/CT496z1.html

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe

Testimony of Todd C. Helmus[1]
The RAND Corporation[2]

Addendum to testimony before the Select Committee on Intelligence
United States Senate

Submitted August 30, 2018

Following the hearing on August 1, 2018, the congressional committee sought additional information and requested answers to the questions in this document. The answers were submitted for the record.

Questions from Senator Tom Cotton

Question 1

As most people are aware, the most detailed accounting of Russia's past activities is the Mitrokhin Archive. On page 243 of the Mitrokhin Archive, as detailed in The Sword and the Shield, it states,

It was the extreme priority attached by the Centre (KGB Headquarters) to discrediting the policies of the Reagan administration which led Andropov to decree formally on April 12, 1982, as one of the last acts of his fifteen-year term as chairman of the KGB, that is was the duty of all foreign intelligence officers, whatever their "line" or department, to participate in active measures. Ensuring that Reagan did not serve a second term thus became Service A's most important objective.

On February 25, 1983, the Centre instructed its three American residences to being planning actives measures to ensure Reagan's defeat in the presidential election of November 1984. They were ordered to acquire contacts on the staffs of all possible presidential candidates and in both party headquarters... The Centre made clear that any candidate, of either party, would be preferable to Reagan.

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

Residences around the world were ordered to popularize the slogan "Reagan Means War!" The Centre announced five active measures "theses" to be used... his militarist adventurism; his personal responsibility for accelerating the arms race; his support for repressive regimes around the world; his responsibility for tension with his NATO allies. Active Measures "theses" in domestic policy included Reagan's alleged discrimination against ethnic minorities; corruption in his administration; and Reagan's subservience to the military-industrial complex."

So, in 1982, over thirty-five years ago, we had the KGB using active measures in the United States to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage. Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

Answer

The focus of the RAND research used as a basis for my testimony before the committee was on Russia's propaganda efforts directed at Eastern Europe. The research for this study was conducted in 2017[3]. That study, as well as my other research, did not review this historical analog in great detail, and thus I cannot compare Russia's campaign against the Reagan presidency, as articulated above, and Russia's modern political warfare campaign against the United States at this time.

Question 2

Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

Answer

It is true that Russia has historically worked to meddle in the internal affairs of various foreign countries. For example, a recent RAND Corporation study highlighted a Russian political warfare campaign in Estonia known as the "Bronze Night," when Russia, in an effort to respond to the Estonian government's quest to move a statue commemorating the Soviet victory in World War II, launched cyber attacks against the country's web domains and possibly organized a major protest that left one dead and 150 injured.[5] According to a recent Center for Strategic and International Studies report, Russia has also cultivated "an opaque web of economic and political patronage" that sought to influence internal politics, state institutions, and economies of

---

[3] Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of August 30, 2018: www.rand.org/t/RR2237

[5] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migazheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018. As of August 30, 2018: www.rand.org/t/RR1772

Hungary, Slovakia, Bulgaria, Latvia, and Serbia.[6] Russia has most certainly sought to assert influence in other nation states as well.

As the question suggests, what is clearly unique about recent Russian political warfare activities is its use of social media. The Kremlin initially developed its army of *trolls* (fake social media accounts managed by Russian agents) and social media *bots* (automated social media accounts) in order to influence the Russian domestic audience.[7] With some apparent success, the Kremlin then began to train these capabilities on foreign audiences, most immediately against Ukraine, and then beyond.

These social media operations, which have also included the use of Facebook ads and pages, are particularly unique and potentially powerful because of their ability to link specific messages with specific target audiences. A simple review of Facebook's capability for ad-targeting illustrates its power as a potential tool for political warfare. Specifically, the medium allows advertisers access to "powerful audience selection tools" that can be used to "target the people who are right for your business."[8] Such tools can increase the efficiency and potential efficacy of messaging campaigns that had, prior to the social media age, not been available at scale to government propaganda campaigns. The social media campaigns can also mimic popular conversations and debates and so exert a kind of peer influence on American audiences. Ensuring that malign actors like Russia do not have easy access to such tools will prove a critical challenge to technology companies and policymakers in the years ahead.

Question 3

We've heard from open testimony before this Committee that the Russians are using active measures to undermine our missile defense deployments, nuclear modernization efforts, and to try and drive a wedge between the U.S. and NATO on these issues. Additionally, we know from Mitrokhin and Bob Gate's memoir "From the Shadows" that this was part of their playbook in the 1980s as well.

To what extent have you looked for and seen Russian activity on this front on social media?

Answer

The focus of the RAND research used in my testimony before the committee was on Russia's propaganda efforts directed at Eastern Europe.[9] As part of that work, we identified and reviewed Russian efforts to drive a wedge between Russian speakers in the Baltics and their home states, the European Union, and members of the North Atlantic Treaty Organization (NATO). However,

---

[6] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: Center for Strategic and International Studies, 2016.

[7] Keir Giles, *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London: Chatham House, Russia and Eurasia Programme, March 2016.

[8] Facebook, "Choose Your Audience," webpage, 2018. As of August 30, 2018: https://www.facebook.com/business/products/ads/ad-targeting

[9] Helmus et al., 2018.

we did not look for or identify Russian efforts to drive a wedge between the United States and NATO.

Questions from Senator Joe Manchin

Question 1

What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

Answer

It seems logical to conclude that if consumers were able to determine whether particular social media content was the direct product of a foreign disinformation or influence campaign, then that content would potentially lose much of its influence value. If an intriguing social media post was outed as a social media bot or identified as coming from a known Russian troll, then that content would seem to lose all credibility. Consequently, the report I co-wrote on the topic, *Russian Social Media Influence*, identified several ways that technology firms or other external entities, such as governments, could inform audiences quickly and directly of Russian propaganda content.

We have previously noted that it is critical to highlight Russian propaganda in ways that are fast and that target at-risk audiences. Thus, our study highlighted several new approaches that could possibly take advantage of advances in modern information technology. For example, our study highlighted the potential use of Google Ads. This approach uses videos and other content embedded in Google search results to educate populations who search for Russian-created fake news on Google and other search engines. The report also highlighted the potential value of viewpoint bots. A viewpoint bot can, in theory, use advanced algorithms to identify Russian bots or trolls engaged in hashtag campaigns. Once it identifies a bot or troll, the viewpoint bot posts messages to the offending hashtags, informing audiences of Russian influence efforts.

However, there may be a need for some caution in the implementation of any disinformation tagging campaign. In 2017, Facebook implemented a campaign to mark inaccurate posts with a "Disputed" tag. However, less than a year after its implementation, Facebook terminated the program because the effort was deemed ineffective.[11] In particular, Facebook's testing revealed that marking some content "false" or "disputed" did not necessarily change some audience members' opinions about the accuracy of the content. And Facebook cited research suggesting that strong language or visualizations, such as the "Disputed" marker, can actually "backfire and further entrench someone's beliefs."[12] Other researchers show what they call an "implied truth" effect, by which "false stories that fail to get tagged are considered validated, and thus are seen

[11] Tessa Lyons, "Replacing Disputed Flags with Related Articles," Facebook, December 20, 2017. As of August 30, 2018:
https://newsroom.fb.com/news/2017/12/news-feed-fyi-updates-in-our-fight-against-misinformation/

[12] Jeff Smith, Grace Jackson, and Seetha Raj, "Designing Against Misinformation," *Medium*, December 20, 2017. As of August 30, 2018: https://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2

as more accurate."13 Consequently, it will be critical to ensure that any new efforts that tag false content undergo empirical evaluations to ensure that the regimens achieve their intended effect.

Question 2

Should there be disclaimers on anything other than personal information?

Answer

Unfortunately, our study on Russian social media operations in Eastern Europe did not address this type of policy response, so I will refrain from answering this question.

Question 3

Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

Answer

Unfortunately, our study on Russian social media operations in Eastern Europe did not address this type of policy response, so I will refrain from answering this question.

Question from Senator Angus King

Question 1

At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:

- *Technical solutions, such as requirements to label bot activity or identify inauthentic accounts;*
- *Public initiatives focused on building media literacy;*
- *Solutions to increase deterrence against foreign manipulation; and*
- *Any additional policy recommendations.*

Answer

While we were conducting field research in Estonia and Latvia and having phone conversations with numerous other regional activists, the recommendation we heard most frequently was the need for media literacy training.

---

[13] Gordon Pennycook and David G. Rand, "The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings," working paper, December 8, 2017. As of August 30, 2018: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035384

Several such efforts in Eastern Europe are currently under way. For example, the Non-Governmental Organization, Media Baltic Centre, with some international funding, provides training to journalists in the Baltics and conducts media literacy training in the region. In addition to helping journalists avoid becoming "unwitting multipliers of misleading information," the organization works with school teachers in the region to help them "decode media and incorporate media research into teaching." The program also works to guide school children with media production programs and help raise awareness of fake news on social media. In addition, the U.S. embassy in Latvia was looking to initiate media literacy programming. A local tech entrepreneur in Latvia is interested in creating a nongovernmental organization start-up that would advocate for broader media literacy training and develop a Baltic-focused, crowdsourced, fact-checking website along the lines of the popular English-language fact-checking site Snopes.[14] Beyond these disparate efforts, we recommended establishing media literacy training as part of a national curriculum. Both Canada and Australia have developed such curriculums. In addition, Sweden, based on concerns of Russian fake news and propaganda, has launched a nationwide school program to teach students to identify Russian propaganda.[155]

Given that a curriculum-based training program will take time to develop and establish impact, we recommended that authorities in Eastern Europe launch a public information campaign that teaches the concepts of media literacy to a mass audience. This campaign, disseminated via conventional and social media, could be targeted to the populations in greatest need. It is likewise possible to meld public information campaigns with social media–driven training programs. Facebook has also launched its own media literacy campaign, most recently marked by distributing tips to users for spotting fake news stories.[15] As we noted, it would certainly be possible to develop such efforts for an East European and Ukrainian audience.

In theory, helping audiences, including those in the United States, better access, analyze, and evaluate media messages and their accuracy can help reduce the plague of fake news and limit the ability of Russia to blindly influence the U.S. public. However, the scientific evidence for media literacy training to help audiences detect the types of content produced by propagandists remains limited. Consequently, for both U.S. and European media literacy initiatives, it will be critical to scientifically evaluate the impact of such initiatives and determine the types of trainings (e.g., online versus offline, short course versus long course) that are suitable for specific audiences, mediums, and content.

---

[14] Helmus et al., 2018.

[15] See, for example, Facebook, "Tips to Spot False News," webpage, 2018. As of August 30, 2018: https://www.facebook.com/help/188118808357379

UNCLASSIFIED

Questions for the Record Senate Select Committee on Intelligence Foreign Influence Operations and Their Use of Social Media Platforms August 1, 2018

Questions for the Record for Renee DiResta

[From Senator Cotton]

As most people are aware, the most detailed accounting of Russia's past activities is the Mitrokhin Archive. On page 243 of the Mitrokhin Archive, as detailed in The Sword and the Shield, it states,

It was the extreme priority attached by the Centre (KGB Headquarters) to discrediting the policies of the Reagan administration which led Adropov to decree formally on April 12, 1982, as one of the last acts of his fifteen-year term as chairman of the KGB, that is was the duty of all foreign intelligence officers, whatever their "line" or department, to participate in active measures. Ensuring that Reagan did not serve a second term thus became Service A's most important objective.

On February 25, 1983, the Centre instructed its three American residences to being planning actives measures to ensure Reagan's defeat in the presidential election of November 1984. They were ordered to acquire contacts on the staffs of all possible presidential candidates and in both party headquarters...The Centre made clear that any candidate, of either party, would be preferable to Reagan.

Residences around the world were ordered to popularize the slogan "Reagan Means War!" The Centre announced five active measures "theses" to be used...his militarist adventurism; his personal responsibility for accelerating the arms race; his support for repressive regimes around the world; his responsibility for tension with his NATO allies. Active Measures "theses" in domestic policy included Reagan's alleged discrimination against ethnic minorities; corruption in his administration; and Reagan's subservience to the military-industrial complex."

1) So, in 1982, over thirty-five years ago, we had the KGB using active measures in the United Stat to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage. Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

Thematically there is some overlap between present day and past KGB active measures messaging; wars and corruption figured in prominently in the content on several Internet Research Agency (IRA)-linked sites. However, the themes that the IRA prioritized in 2018 were primarily internal societal struggles designed to create rifts between subsets of Americans. The tensions the IRA sought to exploit included racial discord (which appeared in numerous forms such as black and white militant and separatist content, Confederacy nostalgia, black culture content, police-violence related content), immigration status, cultural differences, religious

freedom, and hot-button political issues such as gun ownership rights and LGBT rights.

2) Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

The difference is, indeed, the distributor -- and this is a critically important difference. Social networks afford an opportunity for speaking directly to people without the intervention of a gatekeeper; older active measures strategies often included the goal of laundering sympathetic content into a respected publication, but now the distrust in mainstream media affords subversive foreign propagandists the ability to simply market their content as "citizen journalism". In addition, the relatively low cost of online publishing, coupled with the availability of fraudulent social media accounts to share and otherwise elevate that content on highly-trafficked social media platforms, provides for nearly limitless experimentation. Adversaries can test market thousands of divisive narratives simultaneously using state-of-the-art tools for measuring already provided to marketers by the social media platforms.

There is an intersection of three factors at work: consolidation of hundreds of millions of users onto a handful of platforms, gameable algorithms, and the ability for precision targeting of content (designed to facilitate targeted ads in support of the advertising business model). The combination of these factors make it possible to distribute computational propaganda across a dense social ecosystem to those most likely to be receptive to it, and the content often receives an algorithmic assist. User-created content is for the most part treated equally; when it achieves a sufficient number of likes or shares, the platform algorithms may begin to promote it as "trending" or "recommended" content. Social platforms are built to drive user engagement; they are made to facilitate virality, and the ease of sharing ensures a velocity of transmission that makes stopping the spread of disinformation a significant challenge.

This new distribution model enables an unprecedented scale for influence operations and serves as an asymmetric advantage to any mildly sophisticated actor intent on pursuing these goals.

We've heard from open testimony before this Committee that the Russians are using active measures to undermine our missile defense deployments, nuclear modernization efforts, and to try and drive a wedge between the U.S. and NATO on these issues. Additionally, we know from Mitrokhin and Bob Gate's memoir "From the Shadows" that this was part of their playbook in the 1980s as well.

3) To what extent have you looked for and seen Russian activity on this front on social media?

With the caveat that attribution is complex, there are ongoing narratives that attempt to discredit NATO being spread and amplified in Kremlin-linked social media communities. This is

not a new phenomenon; there was press coverage in the New York Times (https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html)

and The Guardian (https://www.theguardian.com/world/2017/jan/11/russia-waging-information-war-in-sweden-study-finds) about Swedish audiences being targeted with anti-NATO messaging in 2016 when Sweden was debating a military partnership with the alliance; the Swedish government identified Russia as the source of the false narratives.

There are also potentially abnormal patterns in the creation data of user accounts on Twitter that are focused on the topic. Among accounts currently discussing NATO on Twitter, we have observed an increase in the number of Twitter accounts brought online over time since the Swedish operation began. Further, the English-language accounts that we have observed sharing broader pro-Russia or Russian-origination messaging are also posting negative things about NATO and the US relationship with NATO allies. This is an ongoing investigation, but it appears that Russia and its surrogates are targeting Americans with messaging meant to call our role in NATO into question.

[From Senator Manchin]

4) What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

There is an information war happening, and multiple types of actors are participating. This includes hostile state and non-state actors, but also includes coordinated attempts to spread disinformation by groups of real American ideologues. The platforms face a challenge in balancing cultural First Amendment expectations and allegations of censorship against the potential damage resulting from the unfettered spread of manipulative narratives designed to cause harm to individuals, society, and businesses alike. We believe that transparency about both the content itself (attribution) and the financial motivations behind it serve the interests of an informed citizenry. However, the ease of anonymous content creation on the internet - anyone can start a blog or make a meme - make identification of the source a significant challenge, and political dark money makes disclosing funding an unwinnable battle in the current legal environment.

What is possible, however, is for social media companies to take dubious distribution patterns into account when deciding what content their algorithms will recommend. Similarly, it is possible to assign quality indicators that factor in past behavior of the accounts sharing it (a 'spamminess', or quality quotient) and to the domain the content resides on. There is precedent for this in the effort to mitigate spam. Platforms should look to the history of anti-spam efforts for inspiration on managing computational disinformation as well.

Recognizing that this is an ongoing information war, we do anticipate an evolution in disinformation tactics from simple botnets to far more sophisticated narrative laundering

through authentic American accounts. Therefore, information sharing between third party researchers and technology platforms provides the best framework for ongoing protection of the information ecosystem.

5) Should there be disclaimers on anything other than personal information?

6) Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

To answer both 5 and 6: content provenance is technologically extremely complex to implement at the scale described in the question, and also not terribly difficult for a determined adversary to evade. Visual image memes in particular often evolve slightly as they spread from user to user, so it's unclear what the attribution would or should link to. Repurposing and amplifying existing content is a tactic we have seen used by both the Internet Research Agency and the newly discovered Iranian social media manipulation operation; much of what they shared came from legitimate American news articles and meme pages, so even precise labeling of the content would not have made a significant impact in uncovering the operation.

[From Senator King]

7) At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:

• Technical solutions, such as requirements to label bot activity or identify inauthentic accounts;

• Public initiatives focused on building media literacy;

• Solutions to increase deterrence against foreign manipulation; and

• Any additional policy recommendations.

The technologies underpinning the social media platforms have evolved in such a way that the interplay between three key phenomena -- mass consolidation of audiences onto a handful of platforms, gameable algorithms, and the ability to easily and precisely target people -- have created a problematic information ecosystem.

Legislating technological solutions for feature-level tactics leveraged by the IRA is fighting the last war. The specific features of social networks evolve rapidly; a Facebook ad today looks very little like an ad did a few years ago. Twitter has already diminished the ability for blocs of fully-automated accounts to easily game trending, so requiring that bots be labeled will have much less of an impact in 2018 than it could have had in 2016. The platforms already have policies in place for taking down inauthentic accounts; public pressure and pressure from financial stakeholders has begun to incentivize them to do so much more proactively. We

advocate avoiding the Maginot line of feature-focused legislation and instead prioritizing:

1) Implementation of cross-platform computational propaganda and algorithmic manipulation detection solutions to enable more rapid discovery of the signatures that indicate an emerging influence operation
2) Establishing oversight mechanisms empowered to keep the social media platforms acting in the interest of the public
3) Creating global economic and military deterrence strategies to raise the cost and risk of conducting influence operations for the malign actors involved.

Senator Warner introduced 20 policy proposals in a whitepaper immediately preceding the August 1 hearing that inspired this inquiry. In line with several of his proposals, we advocate for:

- The granting of rulemaking authority to the FTC as a significant step forward in the creation of a system of social platform oversight
- The establishment of an interagency task force, the creation of a formal deterrence strategy, and a re-evaluation of the Information Operations Doctrine
- The establishment of a public-private standing body to support threat information sharing between government, platforms, and researchers.

There is currently no disincentive to dissuade anyone, foreign or domestic, from undertaking a mass manipulation campaign ahead of an election. It is easy, it is inexpensive, and - judging by the fact that Russian and Iranian operations are still ongoing - past consequences have not yet created a perception that attacking the United States in this way will results in severe repercussions.

The United States presently faces extreme difficulties countering influence operations online because of laws such as US Law 50 U.S. Code § 3093(f), which prohibits the government from counter-messaging or engaging out of fear that such activity might violate the provision that prevents action "intended to influence United States political processes, public opinion, policies, or media." Similarly, there is concern that gathering information, or collecting and analyzing the posts of suspect foreign social media accounts, could potentially violate the 1974 Privacy Act that governs the gathering of information about individuals if an American citizen's information was also inadvertently gathered. These challenges were identified in 2015 while establishing the Global Engagement Center inside the State Department; engaging with presumed-foreign extremist accounts in anything other than an overt attributed capacity was deemed impossible because of the chance that an American digital bystander might see it, or that the pseudonymous extremist was perhaps themselves an American citizen. Therefore, at the moment, the overseas-partner model of the GEC provides the best option for countering foreign propaganda, and it should be fully staffed and funded.

Within the United States, the responsibility for coordinating investigations and responses to

influence operations is presently fragmented across the intelligence community. The CIA and NSA are constrained, leaving the FBI in charge of investigations. In contrast, several of our allies, including Germany and France, have dedicated cybersecurity organizations devoted to defense against these sophisticated attacks. These organizations are technically skilled agencies that are integrated and share intelligence with the rest of the country's national security entities; they have the technological expertise to engage with tech companies around threat information. The United States needs a similar whole-of-government approach to information operations, and must treat the threat as a cybersecurity issue.

Presently, oversight of threats to American democracy by way of private social platform infrastructure might fall under the purview of the Federal Trade Commission or the Federal Election Commission. The FTC has broad consumer-protection responsibilities but has neither deep expertise in internet manipulation, nor rulemaking authority. And since disinformation on the internet includes malign narratives outside of electoral or political concerns, FEC oversight would likely be insufficient. We need to more clearly assign responsibility and ensure that the agency chosen (or created) has the necessary tools to ensure that social networking companies take responsibility for addressing influence operations on their platform.

Domestic efforts must be complimented by an updated global IO doctrine and international detection and deterrence strategy, with the goal of mitigating foreign influence targeting our allies. We need a clear delegation of responsibility for this activity within the U.S. Government. Empowering law enforcement with updated legal tools to investigate and prosecute sophisticated foreign propaganda is essential; we should consider legislation that defines and criminalizes foreign propaganda that targets not just our political process but also addresses the targeting of commercial industry.

To address the final suggested policy area in the question: public initiatives to build media literacy are worth exploring in the interest of helping American citizens better understand how social media works, from the basics of the fact that there is an algorithmic ranking to the specifics of how misinformation and disinformation spread. We believe that any such program would have to apply not only to younger individuals currently enrolled in formal schooling, but to all Americans. One option for this might be a government-sponsored public service media literacy campaign, perhaps sponsored and disseminated on the social platforms in question.

Graphika

RESPONSES TO QUESTIONS FOR THE RECORD
For Senate Select Committee on Intelligence: Foreign Influence Operations and Their Use of Social Media Platforms
Dr. John W. Kelly, Chief Executive Officer
August 30, 2018

Answers for Senator Cotton

Dear Senator Cotton,

I fully agree that current Russian propaganda leverages tactics and themes familiar to history professors. In that regard, it is indeed "old wine." What is new is that in 2018, we manufacture and distribute the bottles. And we do so with a distribution system that is far more effective at delivering tailored Russian messages to specific American audiences.

Contemporary Russian propaganda is distributed to US audiences on American social media platforms, and through American companies. There are both new risks and new opportunities in this scenario. The primary risk is that, as these Russian manipulation strategies are exposed and denounced, American businesses suffer the cost of having been so blatantly manipulated. The opportunity is that, properly harnessed, we can leverage platform data to achieve unprecedented insight into the details of operations designed to manipulate American audiences. As Facebook's recent proactive disclosures show, the current state of affairs enables the ability to detect and disclose influence campaigns before they have an opportunity to further spread.

Answers for Senator Manchin

Dear Senator Manchin,

Foreign influence campaigns on social media are rarely constrained within a single platform, and sophisticated actors are adept at covering their tracks. There is no Russian team with a "Facebook" assignment: rather, we now know (thanks to the excellent academic efforts and investigative journalism in this space) that teams are empowered to influence specific topics (such as the efficiency of vaccines) or audiences (such as African-American activists), and to leverage *all* necessary channels and platforms in doing so.

As a result, large social media companies must cooperate with one another and also empower external experts to detect manipulations and help them understand how they are being

"gamed" by foreign actors and others leveraging similar techniques. This is a problem for the entire technology industry, and it won't be solved in silos constrained by each platforms' specific features and products.

Digital watermarking and other techniques for creating audit trails for content origin might provide some value within a larger strategy, but these alone would prove little more than a speed-bump to manipulators. Alone, these are lightweight "tree solutions," forensics assessments that focus on only one simple aspect of the problem. *Is this tree real or plastic?* In the coming arms race for 21st Century cyber-social warfare, we require "forest solutions," approaches that employ sophisticated large-scale data analysis to detect manipulation at scale across multiple channels and platforms.

We believe that an investment in research and development in this space will yield efficient methods for the detection of foreign manipulation and that those methods will be - as they must be - consistent with American values regarding the protection of user privacy.

Answers for Senator King

Dear Senator King,

Thank you for raising this question, which is focused on the many solutions needed to tackle foreign disinformation. Allow me to reply primarily on the technical front, which is my principal area of expertise.

Leveraging Federal research grants, academic partnerships, and private partnerships with the best and brightest in Silicon Valley, Graphika has already made significant headway in developing frameworks to detect and identify inorganic coordination and messages amplified by both automated and human (bot and troll) online armies. This is not a simple problem, and solving it requires significant investment in network science R&D.

For many years, the detection problem was solely focused on "bots": automated scripts posting social media messages with minimal human intervention. Today, we recognize the problem is more complex than simple automation. Foreign actors, and a growing black market serving their efforts, have developed many techniques to inorganically amplify social media signals in manners more subtle (and harder to detect) than simple bots. This is what Graphika and our partners are mostly focused on now.

Doing this work properly will require that the platforms continue to facilitate access to the types of data needed for researchers and innovators to conduct these analyses and generate new detection models, while ensuring user privacy remains protected.

Questions for the Record
Senate Select Committee on Intelligence
Foreign Influence Operations and Their Use of Social Media Platforms
August 1, 2018

Submitted by Laura M. Rosenberger

1) So, in 1982, over thirty-five years ago, we had the KGB using active measures in the United States to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage. Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

The Russian government - through its intelligence services and proxies like the Internet Research Agency (IRA) - manipulates the information ecosystem to attempt to influence American public opinion and undermine U.S. foreign and domestic policy. These influence operations, which include seizing on hot button or divisive political and social issues, seek to accomplish several objectives: amplify and deepen existing polarization in American politics and society in attempt to weaken the institutional and social fabric of the nation; inject pro-Kremlin geopolitical narratives into public discussion and garner sympathy for them from an American audience; and, weaken and distract the United States from its global responsibilities. While some of the specific issues these operations exploit have evolved since the Cold War – for instance, immigration is a newer divisive issue on which these operations play -- overall the Russian government's objectives in conducting these influence operations are consistent with its Soviet predecessors' aims.

In many instances, Russian influence operations seek to accomplish all three of these objectives simultaneously. The Russian social media campaign around the war in Syria provides a good case study. Several IRA-purchased ads on Facebook attempted to influence American public opinion against U.S. military activity, specifically targeting the Trump administration's May 2017 strikes on Syria.[1] Other ads targeted American liberals frustrated with U.S. military actions in Syria by calling for more focus on domestic issues and describing U.S. leaders as "high-powerful warmongers."[2] One ad purchased by the fake IRA page "Blacktivist" targeted

[1] 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.

[2] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 2426," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

African Americans by asking, "How would we feel if another country bombed us for the poisoned water in Flint and for police brutality?"[3] Others emphasized social issues to criticize U.S. actions in Syria, with one ad using anti-war quotes from Martin Luther King Jr to target civil rights supporters.[4] On Google, English-language searches for key events or players in the Syrian conflict – such as the chemical attacks in Douma or the "White Helmets" civilian rescue organization – regularly returned results dominated by overt Kremlin propaganda outlets pushing conspiracy theories, allowing Moscow to insert its narratives directly into public discussion.[5]

These operations use similar tactics around other geopolitical and divisive issues. IRA accounts on Reddit circulated multiple memes discouraging U.S. support for Montenegrin-accession to NATO. Some posts portrayed Montenegrins as free riders, while others painted them as unwilling participants in the alliance.[6] On Twitter, Russian-linked accounts have similarly promoted negative portrayals of Europe in the U.S. and negative portrayals of the U.S. in Europe to undermine transatlantic bonds.[7] IRA accounts on Twitter have also targeted domestic issues by promoting conspiracy theories,[8] amplifying partisan content related to the NFL anthem protests,[9] and exploiting mass shootings to widen divisions over gun control debates.[10]

In all of these cases, the goal is to polarize domestic U.S. debate and manipulate public opinion on key international issues to further the Kremlin's interests. In this way, social media

---

[3] 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.

[4] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed August 20, 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 August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

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

[6] 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/.

[7] Sophie Eisentraut and Bret Schafer, "Russian Infowar Targets Transatlantic Bonds," *Cipher Brief*, March 30, 2018, https://www.thecipherbrief.com/russian-infowar-targets-transatlantic-bonds.

[8] Salvador Hernandez, "Russian Trolls Spread Baseless Conspiracy Theories Like Pizzagate And QAnon After The Election," BuzzFeed, August 15, 2018, https://www.buzzfeednews.com/article/salvadorhernandez/russian-trolls-spread-baseless-conspiracy-theories-like.

[9] Nicole Einbinder, "The Election Is Over, But Russian Disinformation Hasn't Gone Away," *Frontline*, November 1, 2017, https://www.pbs.org/wgbh/frontline/article/the-election-is-over-but-russian-disinformation-hasnt-gone-away/.

[10] @BEEBCLAPTT, "Sheriff Clarke Sounds Off on Vegas Massacre as Liberals Demand Gun Control https://t.co/FB1EnNda8K," Twitter, October 3, 2017, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

and the online information space have given Moscow an effective way to supercharge its active measures efforts to reach larger audiences at rapid speed for lower costs.

2) Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

In many ways, the playbook employed by the Russian government is similar to the one used by the Soviet-era KGB. The focus on dividing U.S. society by seizing on polarizing domestic issues, inflaming public discussion to undermine American foreign policy, and driving a wedge between the United States and its allies represent continuity in Moscow's strategy to weaken the United States. But while the playbook is in many ways the same, the tools that can be used to run those plays are very different. Digital platforms allow for manipulation of the entire information ecosystem in new and powerful ways, boosting the reach – and possibly the impact – of the playbook. By combining newer digital tactics like automated and inauthentic social media accounts with more traditional tools like state propaganda outlets, the Kremlin can spread its narratives across the information ecosystem to reach a wider audience than ever before and distort the information space itself. Additionally, the anonymity and reach of social media tools has made information operations cheaper, easier, and likely more effective than pre-digital iterations. In the past, conducting widespread information operations required experienced tradecraft and covert distribution networks. Now, basic cultural and linguistic skills, along with an understanding of trending algorithms, is all that is needed for Russian assets to insert narratives into the information space and watch them go viral.[11] The ability to combine these tactics with other cyber means, including to disseminate hacked material obtained through cyberattacks, also enhances the power of this playbook.

3) **To what extent have you looked for and seen Russian activity on this front [to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage] on social media?**

Inauthentic accounts controlled by Russia's Internet Research Agency (IRA) have attempted to influence U.S. defense policy and alliances through a number of methods. For example, numerous ads purchased by IRA accounts on Facebook sought to undermine U.S. policy on Syria, while IRA accounts on Twitter questioned the United States' nuclear capability[12] and commitment to NATO, including tweets asking why Americans would fight and

[11] Andrew Weisburd and Bret Schafer, "Insinuation and Influence: How the Kremlin Targets Americans Online," Alliance for Securing Democracy, October 16, 2017, https://securingdemocracy.gmfus.org/insinuation-and-influence-how-the-kremlin-targets-americans-online/.

[12] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-

die for "Turkey and their Sharia law."[13] Russian-linked accounts on Twitter have also worked to discredit transatlantic partners in the eyes of each other by painting a negative picture of Europe to American audiences and of the United States to European audiences.[14] And IRA accounts on Reddit discouraged U.S. support for Montenegrin-accession to NATO.[15] While I am not aware of specific examples of Russian activity on social media directly targeting U.S. missile defense deployments or nuclear modernization efforts, such messaging would be consistent with the Kremlin's broader goal of weakening our alliances and influencing U.S. policy on geopolitical issues.

4) What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

There are a number of measures that social media platforms can implement to help protect users from foreign manipulation. Most of these measures require greater disclosure and transparency. Online information platforms need to supply users with the context necessary to evaluate the information they encounter, including the origin of content and an explanation of why it is being presented to them. To this end, companies should inform users in a clear and approachable manner how and why certain content appears for them. As outlined in the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*, transparency and disclosure of source information are also essential to protecting the integrity of the U.S. political system.[16] Congress could help promote greater transparency by adopting legislation that improves disclosure requirements for online political advertisements so

---

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 August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.; @RAVENICHOLSON, "Trump questions the US's nuclear arsenal: Here's how the US's nukes compare to Russia's https://t.co/h6KlQ8biha via @BI_Defense," Twitter, December 24, 2016, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

[13] @BEEATRWL, "How heartening is it that our sons and daughters are FIGHTING and DYING for Turkey and their Sharia Law? NATO Turâ€¦ https://t.co/eaQ9QaFWiP," Twitter, August 1, 2017, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

[14] Sophie Eisentraut and Bret Schafer, "Russian Infowar Targets Transatlantic Bonds," *Cipher Brief*, March 30, 2018, https://www.thecipherbrief.com/russian-infowar-targets-transatlantic-bonds.

[15] 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/.

[16] 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

that Americans understand who is funding the political ads they see online, and legislation requiring companies to identify and label automated "bot" accounts.[17]

New mechanisms for data sharing, both between the public and private sectors and among technology companies, are essential for combatting this problem. The U.S. government plays an important role in identifying threat actors of concern, as the intelligence community 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 into activity on their platforms – visibility that government analysts often lack. Information sharing mechanisms between the government and social media platforms should facilitate regular communication of developments on these fronts so that both entities are better positioned to identify, deter, and defend against foreign interference. Additionally, given the manner in which interference operations work across the social media ecosystem, tech companies also need mechanisms in order to regularly share threat indicators with one another. And such data should be shared, with appropriate controls for privacy, with independent researchers. Models of sharing mechanisms between the public and private sectors, cross-industry, and with independent experts exist for counter-terrorism, cybersecurity, and financial integrity.[18]

5) Should there be disclaimers on anything other than personal information?

Context about information is critical for consumers to be able to evaluate it. Users should be able to see and understand the origin of information presented to them, whether the information is being spread by an automated account, and why they are being shown that information. Additionally, there are a variety of ways to require authenticity and provide context without compromising anonymity, which is particularly essential for democratic activists who operate in authoritarian states. Another simple step toward empowering users with contextual information is to label automated accounts, which will help people better understand and evaluate the content they interact with. As outlined in the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Congress could adopt legislation requiring companies to identify and label automated "bot" accounts.[19]

---

[17] 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

[18] 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.

[19] 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

6) Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

Providing users with broader context about the origin of information and why they are seeing it is key to empowering a more discerning and resilient social media culture. As described by Senators Warner and Rubio, "There is really no better defense against Russian aggression on social media than an informed citizenry."[20] Online information platforms should ensure that online content is presented in a manner that relays the origin of the information and why users are seeing the content. Additionally, verifying the authenticity for accounts – while protecting anonymity – and requiring the labeling of automated accounts will help users better understand and evaluate their information environment. Although some platforms have taken steps toward these ends, others have not.

7) What reforms would you recommend to ensure that federal, state and local authorities are not influenced by Russian social media or Internet propaganda?

One of the Kremlin's key objectives with its disinformation campaigns is to cause confusion to slow and undermine the functioning of U.S. institutions. Deception and misdirection are core to its operations to accomplish those objectives. This can include the spread of false or altered documents, as well as the spread of false assertions to undermine U.S. officials' ability to establish a collective truth. No one is entirely immune to covert information manipulation, and it is critical that all Americans scrutinize the sources of their information. The Intelligence Community is well trained at this, and understanding the motivations of sources of information is something that other government officials should be trained on. At a minimum, government employees should be trained to actively verify the sourcing and veracity of information in official material, and should receive up-to-date information from the intelligence community regarding potential nation-state disinformation campaigns. There should also be more formalized partnerships between the various levels of government and the tech platform companies in order to exchange information on foreign attempts to manipulate information online.

8) At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:

---

[20] 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/.

- **Technical solutions, such as requirements to label bot activity or identify inauthentic accounts;**

While I am not a technical expert and defer to such experts on specific recommendations in this area, transparency is a critical principle that should underpin any technical changes. This includes tools to help provide users with more context on the information they are consuming, as well as to label automated accounts. Taking steps to ensure that the algorithms that power these platforms are less vulnerable to manipulation by malicious actors is also critical. Finally, online information platforms should consider the potential utility of hashing as a method or model for identifying and sharing signatures of manipulated or corrupted information.

- **Public initiatives focused on building media literacy;**

Developing media literacy and digital competency programs are key long-term steps to inoculating against the threat of foreign interference. These skills should be taught not only in the classroom, but also through local civil society and non-governmental organizations throughout the country. Some of these organizations are already dedicated to helping Americans better discern sourcing of information, understand why they are seeing it, evaluate whether it may be manipulated, inauthentic, biased, false, or corrupted. These NGOs could partner to conduct public trainings on disinformation and on how to consume news critically; advocate to state and local governments to include media literacy in public education curricula; and devise programs to strengthen civic education, particularly on why democracy matters and why it should be protected against foreign interference. To support these efforts, Congress could establish a fund with pooled public and private resources that would support media and digital literacy education and training throughout the country. This fund could be supported by social media companies as part of their efforts to combat the manipulation of their platforms.[21]

- **Solutions to increase deterrence against foreign manipulation**

Deterrence is essential to securing American democracy against the ongoing threat of foreign interference and preventing adversarial states from conducting future operations. Recent exposure of social media manipulation efforts by Iran,[22] and efforts by China to test these methods, underscore the importance of deterring other authoritarian actors from adopting the Kremlin's playbook.[23] At a basic level, the President of the United States should publicly

---

[21] David Salvo and Brittany Beaulieu, "Ten Legislative Proposals to Defend America Against Foreign Influence Operations," Alliance for Securing Democracy, April 19, 2018, https://securingdemocracy.gmfus.org/ten-legislative-proposals-to-defend-america-against-foreign-influence-operations/.

[22] Casey Michel, "It Turns Out Russia Isn't the Only Country Turning Facebook and Twitter Against Us," *The Washington Post*, August 23, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/08/23/it-turns-out-russia-isnt-the-only-country-turning-facebook-and-twitter-against-us/?noredirect=on&utm_term=.019382e8eac7.

[23] Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance For Securing Democracy, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

articulate a declaratory policy that makes clear the United States considers malign foreign influence operations a national security threat and will respond to them accordingly. Additionally, the Executive Branch should publicly expose and attribute foreign interference efforts as they are discovered – steps by the Department of Justice to adopt such a policy are welcome, and Congress could consider codifying this policy into a mandatory reporting requirement.

To effectively dissuade foreign actors from interfering in our democracy, the U.S. government should tailor its deterrent efforts to most effectively target the interests and weaknesses of foreign regimes while leveraging the United States' relative strengths. In the case of the Russian Federation, the Putin regime is dependent on corrupt financial links between the political leadership, security services, and business for its survival. Inducing behavior change from the Kremlin will require the United States to utilize its relative economic superiority by imposing a broader set of sanctions and reputational costs against individuals and entities that conduct these operations, facilitate corruption, and support authoritarian regimes' destabilizing foreign policy actions.

Additionally, the U.S. should impose reputational costs on authoritarian powers that employ these tools. Vladimir Putin values his standing on the world stage. As such, it is important that Russia not be allowed to reenter normal international fora until Kremlin behavior changes. This is even more relevant for the Chinese Communist Party, which is more sensitive about being exposed for illegal activity and interference operations abroad, as China attempts to sell an alternative model of governance and growth to developing nations.[24] Imposing reputational costs on Beijing must be a pillar of western deterrence strategy.

Finally, the Executive Branch should employ cyber responses as appropriate to respond to cyberattacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats.

- **Any additional policy recommendations**

Effectively countering foreign interference will require a whole of society effort, with actions by government, the private sector, and civil society. For a comprehensive set of policy recommendations for securing U.S. democracy against authoritarian interference, please see the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*.[25] A few specific recommendations are worth highlighting specifically with respect to countering online information manipulation.

New mechanisms for data sharing, both between the public and private sectors and among technology companies, are essential for combatting this problem. The U.S. government

---

[24] Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," Open Forum, The ASAN Forum, May 8, 2018, http://www.theasanforum.org/the-interferenceoperations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response.

[25] 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

plays an important role in identifying threat actors of concern, as the intelligence community 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 into activity on their platforms; visibility that government analysts often lack. Information sharing mechanisms between the government and social media platforms should facilitate regular communication of developments on these fronts so that both entities are better positioned to identify, deter, and defend against foreign interference. Additionally, given the manner in which interference operations work across the social media ecosystem, tech companies also need mechanisms in order to regularly share threat indicators with one another. And such data should be shared, with appropriate controls for privacy, with independent researchers. Models of sharing mechanisms between the public and private sectors, cross-industry, and with independent experts exist for counter-terrorism, cybersecurity, and financial integrity.[26]

This is also a transnational problem, and the United States should develop information sharing and coordination mechanisms with its democratic allies and partners across the transatlantic space and around the world. Actions taken by the U.S. government to punish foreign actors for interference will be much more effective if they are executed in coordination with allies. The G7's recent commitment to share information and work with social media companies and internet service providers to prevent foreign interference in elections is a good first step in this direction, and could serve as an impetus for more efficient transatlantic coordination to share threat information and best practices.[27]

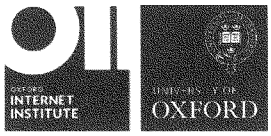
Domestically, the United States should also work to develop better coordination and information-sharing across the U.S. government. Appointing a Counter Foreign Interference Coordinator at the National Security Council and establishing a National Hybrid Threat Center at the Office of the Director of National Intelligence would help the U.S. government work across bureaucratic stovepipes in a unified and coordinated way.[28]

---

[26] 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.

[27] "Charlevoix Commitment on Defending Democracy from Foreign Threats," G7 2018 Charlevoix, June 10, 2018. https://g7.gc.ca/en/official-documents/ charlevoix-commitment-defending-democracy-from-foreign-threats.

[28] A similar concept exists in a bill proposed by Senator Graham and Senator Menendez in August 2018. The "Defending American Security from Kremlin Aggression Act of 2018" calls for the establishment of a "National Fusion Center to Respond to Hybrid Threats," which would coordinate analysis and policy implementation across the U.S. government in responding to hybrid threats. Full text here: https://drive.google.com/file/d/12SoqvkJY8yTLSbUYohzYW978ftpKvCCt/view.



MEMO TO: Senators of the Senate Select Committee on Intelligence
MEMO FROM: Phil Howard, Oxford Internet Institute
MEMO REGARDING: Questions for the Record
MEMO DATE: 04/09/2018

Thank you for the opportunity to respond to more questions. I prefer to stick to the evidence that we in the Project on Computational Propaganda at the Oxford Internet Institute have been collecting and analyzing. So my answers on the long history of Russian propaganda mostly focus on the contemporary trends and evidence that I am familiar with.

Questions from Senator Cotton

1) Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

Some of the themes in today's Russian misinformation campaigns are consistent with previous campaigns, but there are four important differences. First, there are some unusual new themes, many of which are about discouraging voters from trusting evidence, science, or the expertise of their political leaders. For example, there are campaigns to discourage parents in the US from inoculating their kids against diseases. There are campaigns to get people to distrust the science and evidence on things like climate change and healthy nutrition. Second, the propaganda is delivered in a different way. KGB propaganda messages from 30 years ago reached far fewer people, often indirectly, not in a targeted way, and rarely through US media itself. Today, US-based social media companies deliver the content, reaching more people in direct and targeted ways. Third, I think the propaganda attacking two key democratic institutions—journalism and elections—is new. The campaigns to undermine trust in news organizations, independent journalism, elections administrators and public officials are a contemporary phenomenon. Most of the previous Russian propaganda was focused on particular issues and the interpretation of events. This new propaganda is focused on particular democratic processes and institutions. Fourth, the form of political speech is different. US voters had a right to hear the opinions of other governments about world affairs thirty years ago. Contemporary disinformation is so full of lies and disinformation it probably does not warrant the same free speech protections.

2) Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

This metaphor is close but not quite right. The bottles are labelled as wine, but the bottles contain poison and the poison is being distributed over networks of family and friends.

3) To what extent have you looked for and seen Russian activity on this front on social media?

Efforts to undermine trust in the military, nuclear modernization efforts, and sow distrust between the US and NATO continue. But yet another difference is that campaigns of misinformation on national security issues can now be directly targeted at active duty military personnel, veterans, and their friends and family. In our research memo "Junk News on Military Affairs and National Security" we make three observations. First, over Twitter we find that there are significant and persistent interactions between

current and former military personnel and a broad network of extremist, Russia-focused, and international conspiracy subgroups. Second, over Facebook, we find significant and persistent interactions between public pages for military and veterans and subgroups dedicated to political conspiracy, and both sides of the political spectrum. Third, over Facebook, the users who are most interested in conspiracy theories and the political right seem to be distributing the most junk news, whereas users who are either in the military or are veterans are among the most sophisticated news consumers, and share very little junk news through the network.

Questions from Senator Manchin

4) What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

I believe users should have access to two kinds of information: (I) the sources of funding that pay for the ads they see; (II) the ultimate beneficiaries of user data. This means that users should be able to go into their account profile and see a list of the organizations that have paid to place ads directed to them. It means that users should be able to see a list of the third party data mining firms, advertising firms, political actors, and foreign governments that are making use of data the user generated by using the social media platform.

5) Should there be disclaimers on anything other than personal information?

It would be great if users could explore the sources of all ads and content they are served. But this would be a huge volume of information so I believe it best to start with political news, information and ads.

6) Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

Tracking the ultimate source of an ad or post would be interesting to some users. But most people post of the time don't think about politics. They turn to politics when there is an election or crisis brewing, and professional news outlets are working hard to draw public attention to current events.
At election time, or during those sensitive political moments, users are more likely to want to know which lobbyists, political parties, candidates or PACs are benefiting from the data they have generated as users.

Questions from Senator King

7) At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:
    a. Technical solutions, such as requirements to label bot activity or
    b. identify inauthentic accounts;
    c. Public initiatives focused on building media literacy;
    d. Solutions to increase deterrence against foreign manipulation;
    e. Any additional policy recommendations.

There are two ways to protect democracy from the challenge posed by tech companies' dominance over socially valuable data. The first option is for governments to regulate content on an unprecedented scale. That would oblige public regulators to either review all social media content to judge its appropriateness or provide clear signals to private firms — whether the social media companies themselves or third parties — to perform such content reviews. But the problem with both scenarios is that they would create massive new censorship mechanisms that would further threaten democratic culture.

Far preferable would be market regulations that guide firms on how and when they can profit from information about individuals. Such regulations would put the public back in charge of a valuable collective resource while still allowing citizens to express themselves individually by deciding what to do with their data. To get there, policymakers should focus on five basic reforms, all of which would put public institutions back into the flow of data now dominated by private firms.

First, governments should require mandatory reporting about the ultimate beneficiaries of data. That means, when queried, technology firms should be required to clearly report to users which advertisers, data miners, and political consultants have made use of information about them. Your Facebook app or your smart refrigerator should be required to reveal, on request, the list of third parties benefiting from the information the device is collecting. The trail of data should be fully, and clearly, mapped out for users so that if a data-mining firm aggregates users' data and then sells it on to a political party, the users could still identify the ultimate beneficiary.

Second, regulations should require social media platforms to facilitate data donation, empowering users to actively identify the civic groups, political parties, or medical researchers they want to support by sharing data with them. In freeing data from private actors, governments could create an opportunity for civic expression by allowing citizens to share it with whichever organizations and causes they want to support — not just the ones that can afford to buy it, as is the case today. Making data fully portable is only partly about creating some market opportunities for new startups, it is about allowing users to volunteer, participate and engage in a modern way, by contributing to the their data to the civic and public groups they want to support.

The third reform is related to the second: Software and information infrastructure companies should be obliged to tithe for the public good. Ten percent of ads on social media platforms should be reserved for public service announcements, and 10 percent of all user data should be obliged to flow (in a secured way) to public health researchers, civic groups, professional journalists, educators, and public science agencies. Such a system would allow many kinds of advocacy groups and public agencies, beyond the social media firm's private clients, to use existing data to understand and find solutions for public problems.

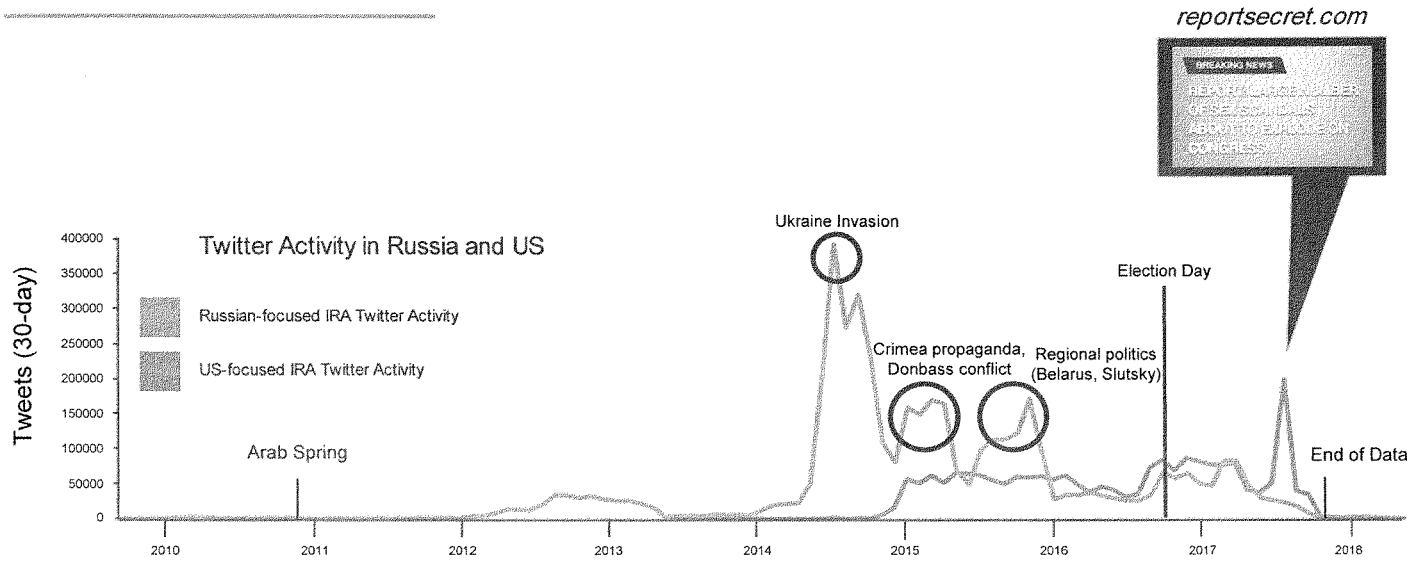
Fourth, the nonprofit rule on data needs to be expanded. Most democracies have rules that prevent firms from profiting from the sale of certain kinds of public data. In many US states, for example, data-mining firms can't profit from the sale of voter registration data, which public agencies collect. This rule needs to be extended to a wider range of socially valuable data, like much of that collected in the US census, but is now gathered and held by technology companies. Such classes of information could then be passed to public agencies, thus creating a broader set of data in the public domain.

Fifth, public agencies should conduct regular audits of social media algorithms and other automated systems that citizens now rely on for information. Technology companies will call these algorithms

proprietary, but public agencies currently audit everything from video gambling machines to financial trading algorithms, all in ways that don't violate intellectual property. Many kinds of political actors have accused technology firms of ideologically biased search and news algorithms. Usually such accusations are baseless, and the deeper problem is misinformation and computational propaganda. Independent review would help us all trust social media and ultimately our political institutions.

Users should have access to clear explanations of the algorithms that determine what news and advertisements they are exposed to, and those explanations should be confirmed by regular public audits. Moreover, all ads, not just political ones, need to be archived for potential use by public investigators. Audits of today's technology would also put the designers of new technologies — such as artificial intelligence — on notice that their own algorithms will one day be under scrutiny.

Russian Focused IRA Efforts vs. US Focused Efforts



The IRA Command & Control: two hands, two gloves

Network is based on account relationships. IP addresses confirm the same operators are manning Right & Left accounts.

Suspended IRA Twitter accounts connected to live accounts on numerous other platforms.

IRA activity: Summary statistics

- The most frequently posted and engaged with websites on Facebook are primarily right-wing partisan sites, and fake sites created by the IRA that targeted African-Americans.
- Sites targeting LGBTQ rights, gun rights, and other contentious issues also received significant focus.
- They made several websites and shared their own content, including blackmattersus.com.

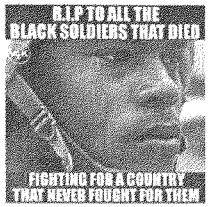
Domain	Count	Engagements
blackmattersus.com	1212	322151
patriotsus.com	89	49939
breitbart.com	62	18953
dailymail.co.uk	12	9735
petitions.whitehouse.gov	5	5738
dailycaller.com	16	3687
youtube.com	99	2973
ny1.com	1	2805
angrypatriotmovement.com	2	2756
usherald.com	2	2712
ihavethetruth.com	1	2217
pinknews.co.uk	11	2195
fwact.org	1	2096
yesimright.com	1	2047
washingtonexaminer.com	10	2014
bluelivesmatter.blue	3	1893
conservativedailypost.com	3	1812
madworldnews.com	4	1666
commonsense.leadpages.co	1	1659
ktxs.com	1	1655

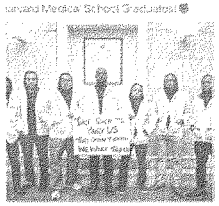
IRA Top Performers: Image Themes

Instagram

Anti-Hillary
Racial

Pro-Gun
Veterans
Religion

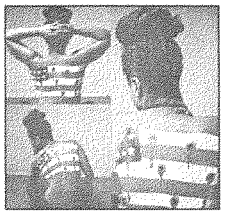


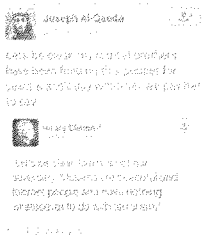


Twitter

Anti-Hillary
Racial

Pro-Trump
Veterans
Anti-Muslim



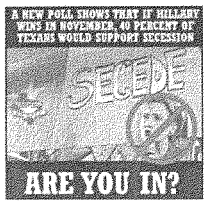


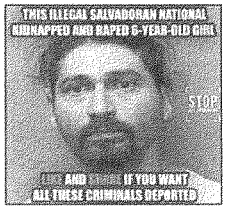
Facebook

Anti-Immigrant
Texas

Patriotic
Veterans

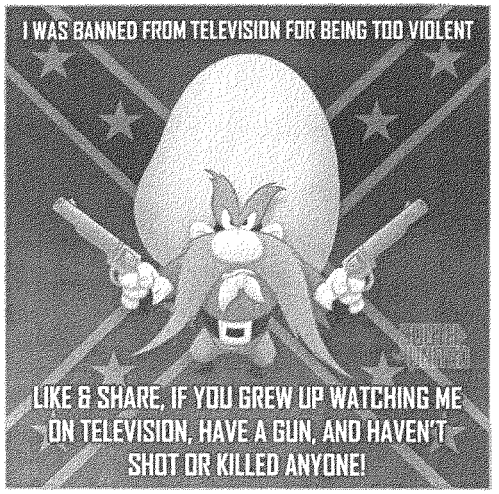
Anti-Muslim





Top Individual IRA Performers: Facebook Content

This March 9, 2016, **South United** meme was the most-shared post on Facebook and had 986,203 total engagements, the most for a single piece of content.



This **Being Patriotic** homeless veterans meme on September 8, 2016 had 723,750 total engagements on Facebook.

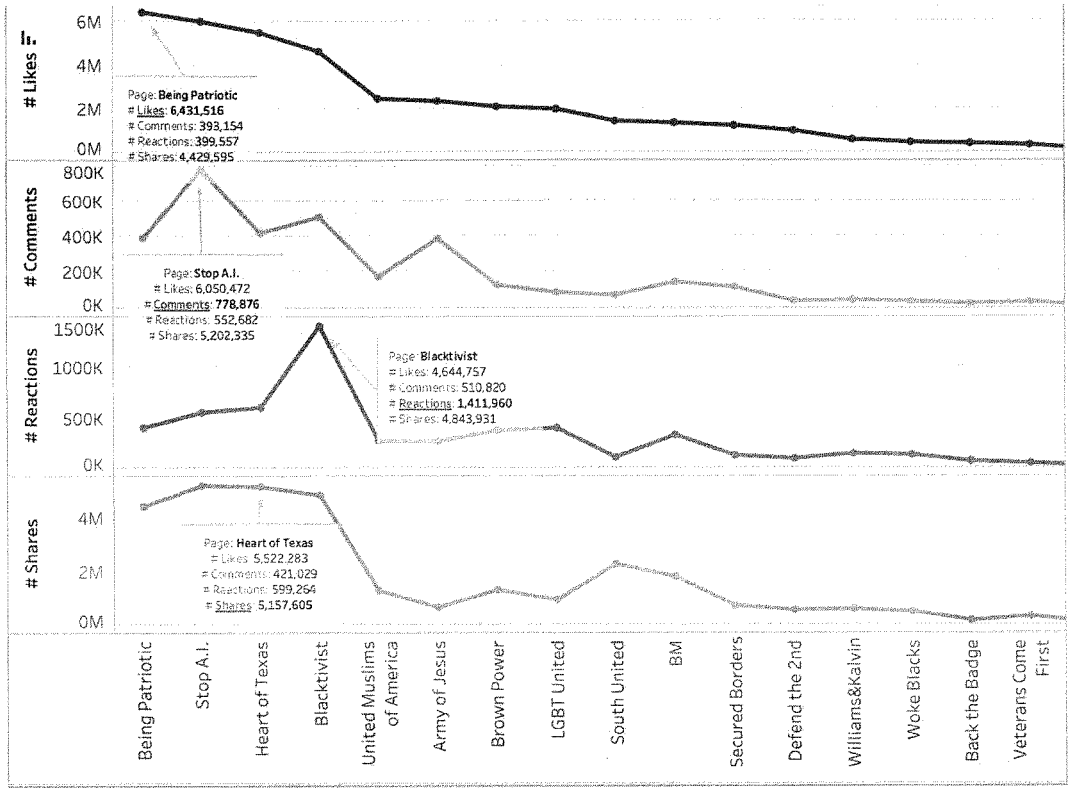
Top IRA Performers: Facebook Accounts

Likes:
Being Patriotic (6.4M)

Comments:
Stop A.I (778k)

Reactions:
Blacktivist (4.6M)

Shares:
Heart of Texas (5.1M)



IRA: Top 20 Domains Shared by Engagement (on Facebook)

1 through 10

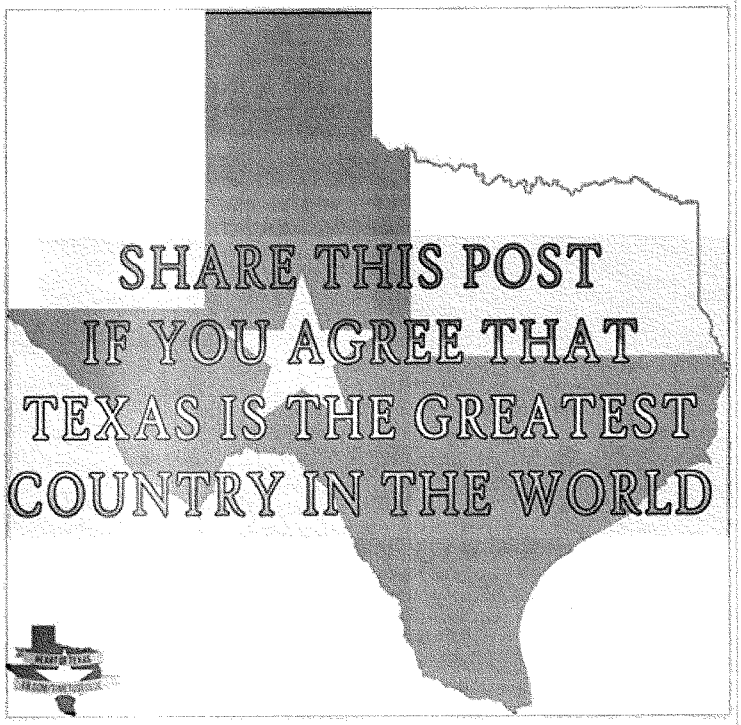
domain	shares	likes	reactions	fb_engagements
blackmattersus.com	100092	142923	58469	301484
patriotsus.com	7372	38361	9109	54842
breitbart.com	4660	11680	4914	21254
dailymail.co.uk	4927	10285	1651	16863
petitions.whitehouse.gov	641	4725	407	5773
angrypatriotmovement.com	1006	3149	439	4594
youtube.com	1087	2237	1026	4350
dailycaller.com	939	2149	839	3927
usherald.com	821	1818	528	3167
ktxs.com	0	2811	354	3165

11 through 20

domain	shares	likes	reactions	fb_engagements
brexitwatch.com	1737	468	696	2901
ny1.com	638	1918	178	2734
therebel.media	1262	804	618	2684
heatst.com	476	2050	112	2638
pinknews.co.uk	336	1152	1131	2619
salamerica.com	0	2286	224	2510
fwact.org	652	1080	730	2462
represent.com	289	1983	180	2452
nation.foxnews.com	943	1044	416	2403
washingtonexaminer.com	431	1237	533	2201

Heart of Texas

Texas deserves to become an independent Republic of Texas again!

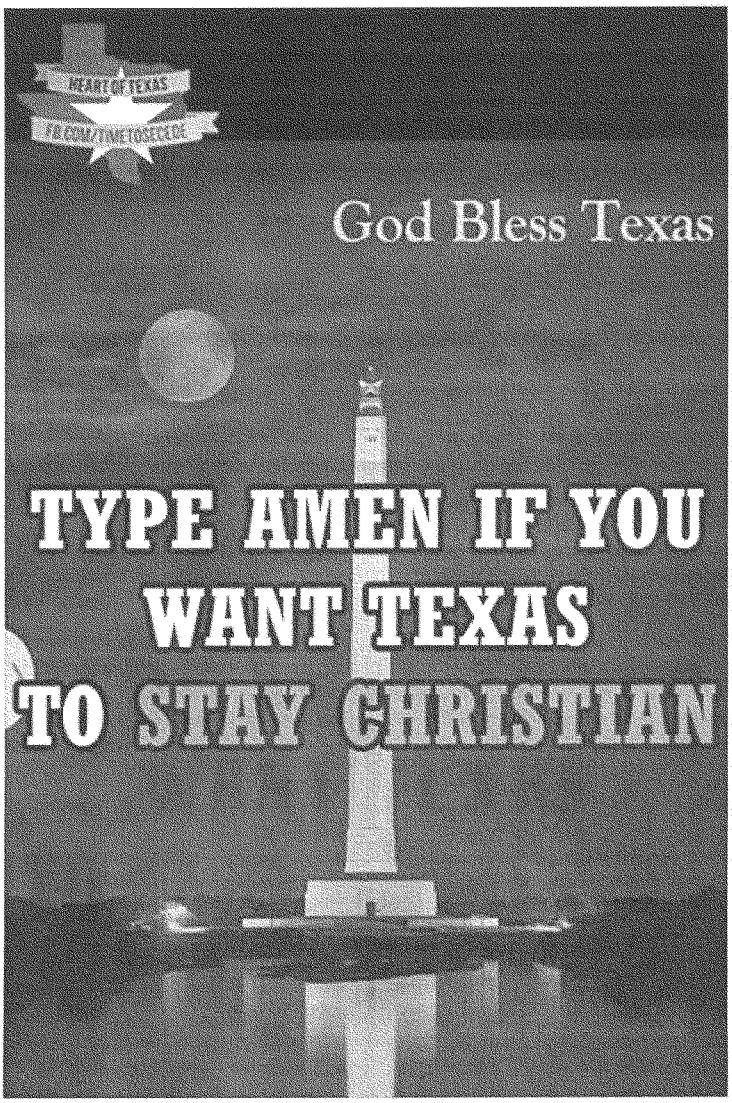


3.2K 118 Comments 25K Shares

Heart of Texas

America's slowly but surely shifting towards turning into islamic state. Our president and our government are pro-islamic and don't want America to believe in our one and only Lord Jesus Christ. Texas will never keep step with U.S.

Texas stays Christian even when odds are against us.



14K 9.6K Comments 20K Shares

Stop A.I.

"Religious" face coverings are putting American people at huge risk! We must not sacrifice national security to satisfy the demands of minorities.

All face covering should be banned in every state across America!

14K 5K Comments 4.3K Shares

Being Patriotic

We're facing attacks on our flags over and over. And believe me – taking our flags away from public places and erasing the heroes' names from our history is just the beginning. Just like attacks on our Second Amendment, the war on flags is nothing but a step to tyranny. We'll never give away our flags, our guns and our faith. God bless our America and every sacred symbol of our country.

11K 662 Comments 15K Shares

Heart of Texas

The Office of the Texas Governor is offering a cash reward up to $15,000 for information leading to the arrest of anyone connected to the execution of the San Antonio officer this past weekend. This reward will be combined to bring the total reward up to $25,000.

The person who executed the officer had initially been described as a clean shaven black man who is approximately 5 feet 7 inches to 6 feet tall. Information has been updated to reflect that the man had a beard. He was wearing a hoodie, baggy pants, and a gray shirt.

In order to be eligible for the cash reward, anyone with information can provide anonymous tips by:

- Calling the San Antonio Crime Stoppers hotline at 210-224-STOP (7867).
- Calling the Texas Crime Stoppers hotline at 1-800-252-TIPS (8477).
- Texting the letters "DPS" followed by your tip to 274637 (CRIMES) from your cell phone.
- Submitting a tip online https://www.tipsubmit.com/WebTipsCSI.aspx?L=E&AgencyID=650

368 8 Comments 135 Shares