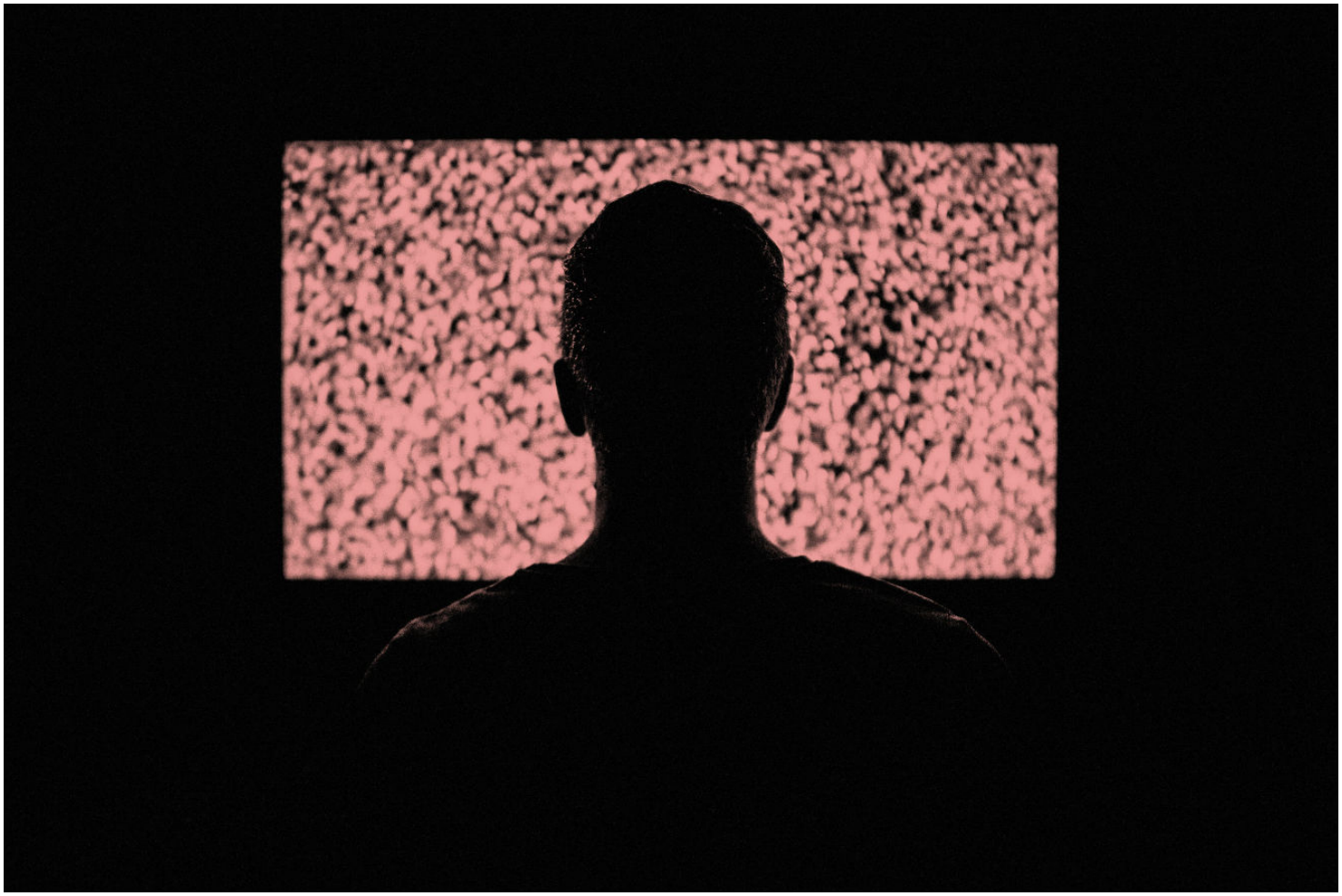
Trolling for Trump: How Russia Is Trying to Destroy Our Democracy

warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/

6-11-2016



In spring 2014, a funny story crossed our social media feeds. A petition on whitehouse.gov called for "sending Alaska back to Russia," and it quickly amassed tens of thousands of signatures. The media ran a number of amused stories on the event, and it was quickly forgotten.

The petition seemed odd to us, and so we looked at which accounts were promoting it on social media. We discovered that thousands of Russian-language bots had been repetitively tweeting links to the petition for weeks before it caught journalists' attention.

Those were the days. Now, instead of pranking petitions, Russian influence networks online are interfering with the 2016 U.S. election. Many people, especially Hillary Clinton supporters, believe that Russia is actively trying to put Donald Trump in the White House.

And the evidence is compelling. A range of activities speaks to a Russian connection: the theft of emails from the Democratic National Committee and Clinton campaign officials, hacks surrounding voter rolls and possibly election machines, Putin's overt praise for Trump, and the curious Kremlin connections of Trump campaign operatives Paul Manafort and Carter Page.

But most observers are missing the point. Russia is helping Trump's campaign, yes, but it is not doing so solely or even necessarily with the goal of placing him in the Oval Office. Rather, these efforts seek to produce a divided electorate and a president with no clear mandate to govern. The ultimate objective is to diminish and tarnish American democracy. Unfortunately, that effort is going very well indeed.

Russia's desire to sow distrust in the American system of government is not new. It's a goal Moscow has pursued since the beginning of the Cold War. Its strategy is not new, either. Soviet-era "active measures" called for using the "force of politics" rather than the "politics of force" to erode American democracy from within. What *is* new is the methods Russia uses to achieve these objectives.

We have been tracking Russian online information operations since 2014, when our interest was piqued by strange activity we observed studying online dimensions of jihadism and the Syrian civil war. When experts published content criticizing the Russian-supported Bashar al Assad regime, organized hordes of trolls would appear to attack the authors on Twitter and Facebook. Examining the troll social networks revealed dozens of accounts presenting themselves as attractive young women eager to talk politics with Americans, including some working in the national security sector. These "honeypot" social media accounts were linked to other accounts used by the Syrian Electronic Army hacker operation. All three elements were working together: the trolls to sow doubt, the honeypots to win trust, and the hackers (we believe) to exploit clicks on dubious links sent out by the first two.

The Syrian network did not stand alone. Beyond it lurked closely interconnected networks tied to Syria's allies, Iran and Russia. Many of these networks were aimed at U.S. political dissenters and domestic extremist movements, including militia groups, white nationalists, and anarchists.

Today, that network is still hard at work, running at peak capacity to destroy Americans' confidence in their system of government. We've monitored more than 7,000 social media accounts over the last 30 months and at times engaged directly with them. Trump isn't the end of Russia's social media and hacking campaign against America, but merely the beginning. Here is what we've learned.

The Russian Social Media Approach: Soviet Union's "Active Measures" On Steroids

The United States and its European allies have always placed state-to-state relations at the forefront of their international strategies. The Soviet system's effort to undermine those relations during the Cold War, updated now by modern Russia, were known as "active measures."

A June 1992 U.S. Information Agency report on the strategy explained:

> *It was often very difficult for Westerners to comprehend this fundamentally different Soviet approach to international relations and, as a result, the centrality to the Soviets (now Russians) of active measures operations was gravely underappreciated.*

Active measures employ a three-pronged approach that attempts to shape foreign policy by directing influence in the following ways: state-to-people, people-to-people, and state-to-state. More often than not, active measures

sidestep traditional diplomacy and normal state-to-state relationships. The Russian government today employs the state-to-people and people-to-people approaches on social media and the internet, directly engaging U.S. and European audiences ripe for an anti-American message, including the alt-right and more traditional right-wing and fascist parties. It also targets left-wing audiences, but currently at a lower tempo.

Until recently, Western governments focused on state-to-state negotiations with Putin's regime largely missed Russian state-to-people social media approaches. Russia's social media campaigns seek five complementary objectives to strengthen Russia's position over Western democracies:

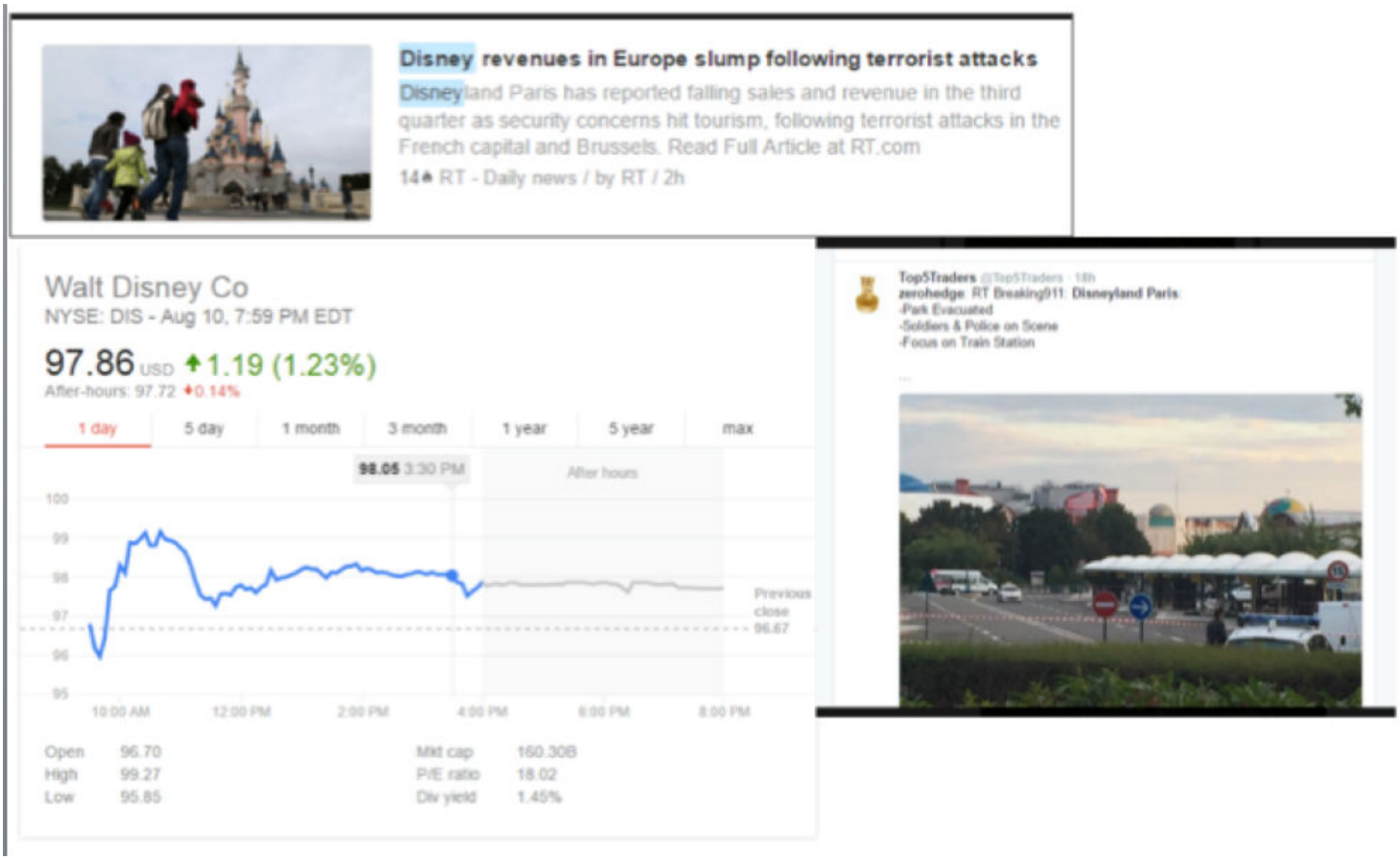
- Undermine citizen confidence in democratic governance;
- Foment and exacerbate divisive political fractures;
- Erode trust between citizens and elected officials and democratic institutions;
- Popularize Russian policy agendas within foreign populations;
- Create general distrust or confusion over information sources by blurring the lines between fact and fiction

In sum, these influence efforts weaken Russia's enemies without the use of force. Russian social media propaganda pushes four general themes to advance Moscow's influence objectives and connect with foreign populations they target.

Political messages are designed to tarnish democratic leaders or undermine institutions. Examples include allegations of voter fraud, election rigging, and political corruption. Leaders can be specifically targeted, for instance by promoting unsubstantiated claims about Hillary Clinton's health, or more obviously by leaking hacked emails.

Financial propaganda weakens citizen and investor confidence in foreign markets and posits the failure of capitalist economies. Stoking fears over the national debt, attacking institutions such as the Federal Reserve, and attempts to discredit Western financial experts and business leaders are all part of this arsenal.

In one example from August, Disneyland Paris was the site of a reported bomb scare. Social media accounts on Twitter reported that the park had been evacuated, and several news outlets — including Russian propaganda stations *RT* and *Sputnik* — published alarming stories based on the tweets, which escalated in hysteria as the afternoon stretched on. In fact, the park had not been evacuated. But that didn't stop Disney's stock from taking a temporary hit. This fluctuation could be exploited by someone who knew the fake scare was coming, but we do not have access to the data that would allow us to know whether this happened.



Social issues currently provide a useful window for Russian messaging. Police brutality, racial tensions, protests, anti-government standoffs, online privacy concerns, and alleged government misconduct are all emphasized to magnify their scale and leveraged to undermine the fabric of society.

Finally, wide-ranging conspiracy theories promote ***fear of global calamity*** while questioning the expertise of anyone who might calm those fears. Russian propaganda operations since 2014 have stoked fears of martial law in the United States, for instance, by promoting chemtrails and Jade Helm conspiracy theories. More recently, Moscow turned to stoking fears of nuclear war between the United States and Russia.

For the Kremlin, this is not just focused on the outside world. Russian news organizations bombard Russian citizens with the same combination of content. Steve Rosenberg, a *BBC News* correspondent in Moscow, filmed the Russian domestic equivalent of this approach on November 1, showing Russian language news headlines inciting fears such as impending nuclear war, a U.S.-Russia confrontation in Syria, and the potential for an assassination of Donald Trump.

The Confluence of Information and Cyberspace

Russian active measures use a blend of overt and covert channels to distribute political, financial, social, and calamitous messages (see above). During the Soviet era, "white" active measures were overt information outlets directly attributable to the Central Committee of the Communist Party of the Soviet Union. Today, *RT* and *Sputnik* push Kremlin-approved English-language news on television and the Internet. These outlets broadcast a mix of true information (the vast majority of content), manipulated or skewed stories, and strategically chosen falsehoods. *RT's* slogan, "Question More," aptly fits their reporting style — seeding ideas of conspiracy or wrongdoing without actually proving anything.

This "white" content provides ammunition for "gray" measures, which employ less overt outlets controlled by Russia, as well as so-called useful idiots that regurgitate Russian themes and "facts" without necessarily taking direction from Russia or collaborating in a fully informed manner.

During the Cold War, gray measures used semi-covert Communist parties, friendship societies, and non-governmental organizations to engage in party-to-party and people-to-people campaigns. Today, gray measures on social media include conspiracy websites, data dump websites, and seemingly credible news aggregators that amplify disinformation and misinformation.

Conspiracy sites include outlets such as InfoWars and Zero Hedge, along with a host of lesser-known sites that repeat and repackage the same basic content for both right- and left-wing consumers. Sometimes, these intermediaries will post the same stories on sites with opposite political orientations.

Data dump websites, such as Wikileaks and DC Leaks, overtly claim to be exposing corruption and promoting transparency by uploading private information stolen during hacks. But the timing and targets of their efforts help guide pro-Russian themes and shape messages by publishing compromising information on selected adversaries.

The people who run these sites do not necessarily know they are participants in Russian agitprop, or at least it is very difficult to prove conclusively that they do. Some sites likely receive direct financial or operational backing, while others may be paid only with juicy information.

Sincere conspiracy theorists can get vacuumed up into the social networks that promote this material. In at least one case, a site described by its creator as parody was thoroughly adopted by Russian influence operators online and turned into an unironic component of their promoted content stream, at least as far as the network's targeted "news" consumers are concerned.

A small army of social media operatives — a mix of Russian-controlled accounts, useful idiots, and innocent bystanders — are deployed to promote all of this material to unknowing audiences. Some of these are real people, others are bots, and some present themselves as innocent news aggregators, providing "breaking news alerts" to happenings worldwide or in specific cities. The latter group is a key tool for moving misinformation and disinformation from primarily Russian-influenced circles into the general social media population. We saw this phenomenon at play in recent reports of a second military coup in Turkey and unsubstantiated reports of an active shooter that led to the shutdown of JFK Airport. Some news aggregators may be directly controlled by Russia, while other aggregators that use algorithmic collection may be the victims of manipulation.

"Black" active measures are now easier to execute than they were for the Soviets. During the Cold War, according to the 1992 USIA report, these included:

> *… the use of agents of influence, forgeries, covert media placements and controlled media to covertly introduce carefully crafted arguments, information, disinformation, and slogans into the discourse in government, media, religious, business, economic, and public arenas in targeted countries.*

Black active measures create both risks and costs. Agents deployed into the West must avoid detection or risk state-to-state consequences. The KGB's Cold War efforts to keep these operations secret bore significant financial costs while producing little quantifiable benefit. Stories were difficult to place in mainstream media outlets, and the slow process made it challenging to create momentum behind any one theme.

On social media, this process is far easier, more effective, and relatively difficult to attribute. Without stepping foot in America, Russia's coordinated hackers, honeypots, and hecklers influence Americans through people-to-people engagement.

Hackers provide the fuel for themes and narratives. Initially, hackers concentrated on defacements, denial of service, and misinformation posted on compromised social media accounts. By 2015, the Kremlin's hacking efforts were much more sophisticated, coalescing into two distinct, competing hacking collectives: Fancy Bear (APT 28), possibly operated by Russian military intelligence (GRU), and Cozy Bear (APT 29), possibly operated by Russia's foreign intelligence service (FSB).

The most notorious Russian-linked hacker, using the handle Guccifer2.0, targets current and former U.S. government officials, American security experts, and media personalities by seeking access to their private communications and records. Former Secretary of State Colin Powell and Clinton campaign chairman John Podesta provide two current examples, but there will be many more to come. Today, Guccifer2.0 posts threats of election meddling this coming Tuesday.


I'd like to warn you that the Democrats may rig the elections on November 8. This may be possible because of the software installed in the FEC networks by the large IT companies.

As I've already said, their software is of poor quality, with many holes and vulnerabilities.

I have registered in the FEC electronic system as an independent election observer; so I will monitor that the elections are held honestly.

I also call on other hackers to join me, monitor the elections from inside and inform the U.S. society about the facts of electoral fraud.

Guccifer 2.0 Warning on Election Posted to Social Media

In addition to phishing and cracking attacks, these hackers are aided by honeypots, a Cold War term of art referring to an espionage operative who sexually seduced or compromised targets. Today's honeypots may include a component of sexual appeal or attraction, but they just as often appear to be people who share a target's political views, obscure personal hobbies, or issues related to family history. Through direct messaging or email conversations, honeypots seek to engage the target in conversations seemingly unrelated to national security or political influence.

These honeypots often appear as friends on social media sites, sending direct messages to their targets to lower their defenses through social engineering. After winning trust, honeypots have been observed taking part in a range of behaviors, including sharing content from white and gray active measures websites, attempting to compromise the target with sexual exchanges, and most perilously, inducing targets to click on malicious links or download attachments infected with malware.

One of us directly experienced how social media direct messages from hackers or influencers seek to compromise or sway a target by using social engineering to build a rapport. Operators may engage the target's friends or acquaintances, drawing them into conversations to encourage trust. Once conversations are started, an agent of influence will be introduced into the group and will subsequently post on Russian themes from grey outlets or introduce malicious links.

When targets click on malicious links, Fancy Bear and Cozy Bear extract personal information from public officials, media personalities, and American experts and selectively dump the content obtained at opportune times. The goal is to increase popular mistrust of political leaders and people with expertise or influence in specific circles of interest to Russia, such as national security. In some cases, experts criticizing Russia have had their computers mysteriously compromised by destructive malware and their research destroyed.

Online hecklers, commonly referred to as trolls, energize Russia's active measures. Ringleader accounts designed to look like real people push organized harassment — including threats of violence — designed to discredit or silence people who wield influence in targeted realms, such as foreign policy or the Syrian civil war. Once the organized hecklers select a target, a variety of volunteers will join in, often out of simple antisocial tendencies. Sometimes, they join in as a result of the target's gender, religion, or ethnic background, with anti-Semitic and misogynistic trolling particularly prevalent at the moment. Our family members and colleagues have been targeted and trolled in this manner via Facebook and other social media.

Hecklers and honeypots can also overlap. For instance, we identified hundreds of accounts of ostensibly American anti-government extremists that are actually linked to Russian influence operations. These accounts create noise and fear, but may also draw actual anti-government extremists into compromising situations. Based on our observations, the latter effort has not been widely successful so far among anti-government extremists, who tend to

stay in their own social networks and are less likely to interact with Russian influence accounts, but our analysis points to greater overlap with networks involving American white nationalists.

Russia's honeypots, hecklers, and hackers have run amok for at least two years, achieving unprecedented success in poisoning America's body politic and creating deep dissent, including a rise in violent extremist activity and visibility. Posting hundreds of times a day on social media, thousands of Russian bots and human influence operators pump massive amounts of disinformation and harassment into public discourse.

This "computational propaganda," a term coined by Philip Howard, has the cumulative effect of creating Clayton A. Davis at Indiana University calls a "majority illusion, where many people appear to believe something ….which makes that thing more credible." The net result is an American information environment where citizens and even subject-matter experts are hard-pressed to distinguish fact from fiction. They are unsure who to trust and thus more willing to believe anything that supports their personal biases and preferences.

The United States disbanded the U.S. Information Agency after the Cold War and currently fields no apparatus to detect and mitigate Russia's social media influence campaign. As seen in America's disjointed counter narratives against the Islamic State, efforts to create any kind of U.S. information strategy are plagued by disparate and uncoordinated efforts strewn among many military, diplomatic, and intelligence commands. American cyber operations and hacking reside separately with the National Security Agency. Russia, on the other hand, seamlessly integrates the two efforts to devastating effect.

After Election Day: What to do about Russia's Active Measures?

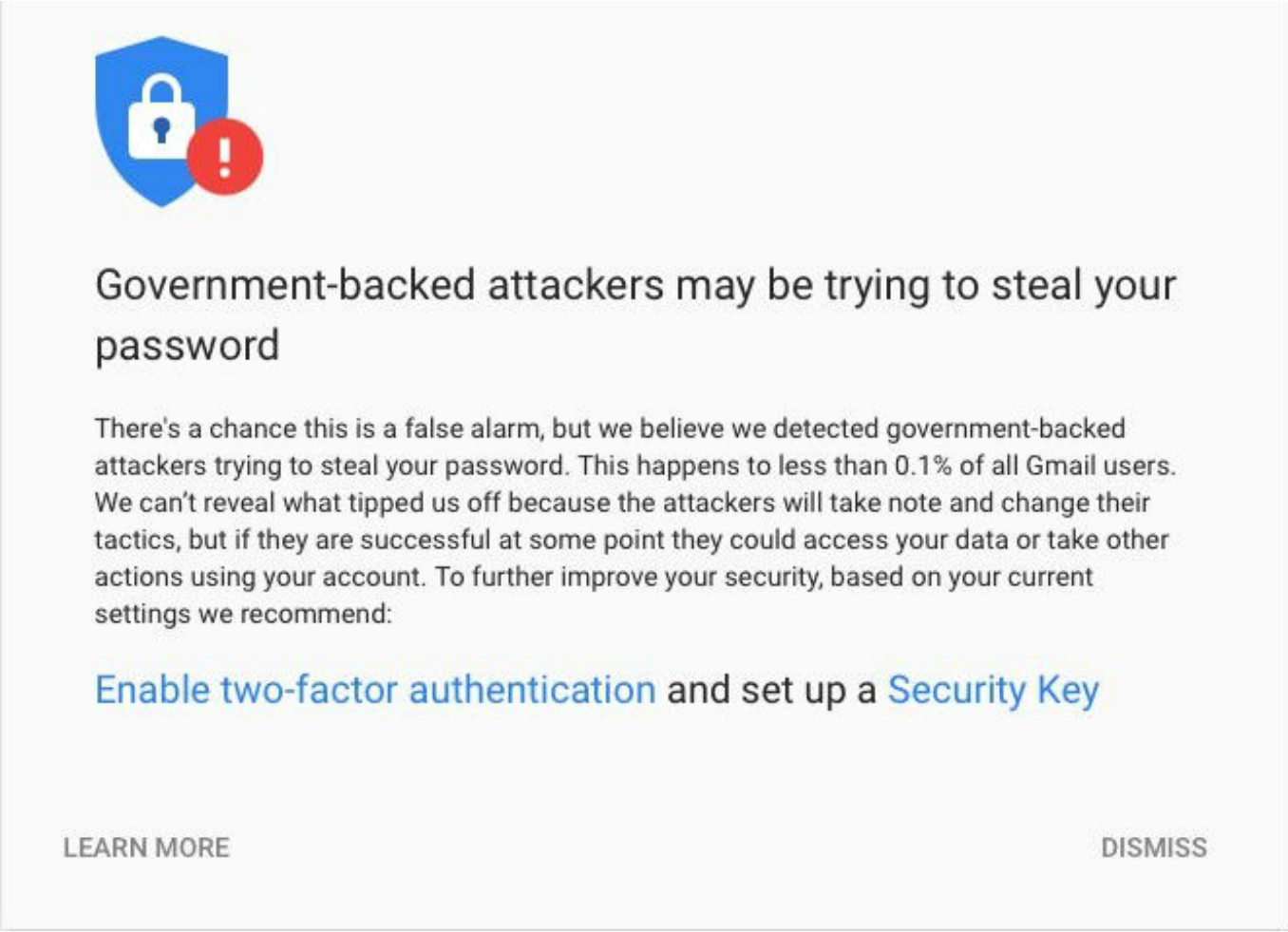
The most overwhelming element of Russia's online active measures over the last year relate to the presidential campaign of Donald Trump. Russian promotion of Trump not only plagues Clinton, but likely helped sideline other GOP candidates in early 2016 with a more traditional anti-Russia view of foreign policy. It is impossible to assess whether Donald Trump is even fully aware of these efforts, let alone complicit. Setting aside that question for a moment, some readers will immediately ask how we are so sure all this activity goes back to Russia?

There are a number of technical indicators, most tellingly the synchronization of messaging and disinformation with "white" outlets such as *RT* and *Sputnik*, as well as the shocking consistency of messaging through specific social networks we have identified.

Dmitri Alperovich of the cyber-security firm Crowdstrike first attributed the DNC hacks to Russia. He explained in a recent *War on the Rocks* podcast:

> *The important thing about attribution…is that it's not that much different from the physical world. Just like someone can plan a perfect bank heist and get away with it, you can do that in the cyber-domain, but you can almost never actually execute a series of bank heists over the course of many years and get away with it. In fact, the probability of you not getting caught is miniscule. And the same thing is true in cyber-space because eventually you make mistakes. Eventually you repeat tradecraft. It's hard to sort of hide the targets you're going after…*

There are other, less subtle indications as well, for instance, a notification from Google: "We believe we detected government backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users." When one of us receives these messages, we feel confident we're on the right trail.



For his part, Trump rejects the idea that Russia is involved and claims it is impossible to know either way. Shane Harris commented:

> *It is startling how he is the only one, it seems, who does not want to acknowledge what 17 intelligence agencies and a lot of technical experts all agree on and his insistence that it could be anyone just flies in the face of the available evidence.*

Trump's business ties to Russia and those of his key advisers have been documented by several journalists, including Harris, who reported that Republican officials were blocking efforts to investigate ties between Trump and Russia.

Regardless of the extent of Trump's direct knowledge about Russia's intelligence activities, active measures have achieved enormous success on the back of his presidential campaign. Russia sees Trump as a tool to undermine its American adversaries. In that regard, they've already achieved their goal and possess the potential to exceed their expectations. As noted previously, the goal of these efforts may not be to elect Trump as president, but rather to ensure the election result is as divided and negative as possible, as reflected in historically low approval ratings for both candidates.

A Trump victory could pave the way for Russian ascendance and American acquiescence, but the candidate's unpredictability may carry more risk than Vladimir Putin would prefer. It is one thing to stoke fears of nuclear war; it is entirely another to risk the actuality. A Trump loss may be adequately beneficial to Russia in the short-term and of even greater benefit over the long term, particularly if the candidate indulges his not-so-veiled hints that he could

engage in an ongoing battle to tarnish the legitimacy of the electoral system. A Trump loss may lead to a Trump television and social media venture, a vehicle to sustain his supporters' angst and perhaps ultimately becoming a high-profile gray active measures outlet.

There are many possible scenarios for the future direction of Russian active measures. Additional damaging information may have been withheld from documented hacks of U.S. political actors, and as-yet undisclosed information — perhaps from a hack of Republican Party emails already suggested by some media reports— may emerge after the election regardless of who wins. Should Russia conduct such data dumps through Wikileaks, for instance, it would create an appearance of balance while also damaging the Republican Party, which almost certainly has at least as much embarrassing material as the DNC. Regardless of who wins, Russian operators might save particularly damaging information for release after the inauguration, when talk of impeachment could further diminish his or her influence in Washington and abroad.

Globally, the implications of Russia's social media active measures are dire. Social media has played a key role in controversial decisions such as Brexit, and in politics and elections around the world, including those of France, Estonia and Ukraine. In heated political contests such as Brexit and the U.S. presidential election, Russian social media active measures could tip the balance of an electoral outcome by influencing a small fraction of a voting public.

Russian employment of bots and covert personas spells trouble for social media companies, too. Their aggressive behavior erodes trust between consumers and the platforms they enjoy. Social media users will not be sure what to believe or who to trust, and they will either limit their sharing or leave social media life altogether after harassment and misinformation. Mainstream media should also reflect on having fallen victim to Russian propaganda time and again in such a way that has made them accomplices to the Kremlin's efforts to damage the American body politic. They can claim to be unwitting accomplices, but given all of the public information on the nature of this Russian information warfare campaign, such claims lack credibility.

The Obama administration has been slow to assess and respond to Russia's social media manipulation, so Russia continues to push the envelope. The U.S. government will need to rapidly develop a strategy to mitigate Russian active measures starting in January 2017. How and when will they counter Russian aggression online? How will they protect citizens from influence operations and hacks? How should we respond to and ultimately deter interference with U.S. elections and the hacking of officials, companies, or citizens?

Meanwhile, the story continues. In late October 2016, Kremlin-linked accounts and bots once again began pushing a White House petition, this time to "remove George Soros-owned voting machines from 16 states." Of course, no such machines exist, but that didn't prevent the petition from racking up nearly 129,000 signatures.

But don't forget about Alaska.

In November 2015, Russian television aired a program arguing that the transfer of Alaska to the United States was invalid. In October 2016, The New York Observer — a newspaper owned by Donald Trump's son-in-law Jared Kushner — published a story about Putin's desire to reclaim Alaska for Russia. Well, at least they can point to that totally legitimate petition.

Andrew A. Weisburd is a Fellow at the Center for Cyber & Homeland Security, a provider of instruction and expert services to the intelligence community, and a non-sworn law enforcement professional.

Clint Watts is a Fox Fellow at the Foreign Policy Research Institute in Philadelphia and a Senior Fellow at the Center for Cyber and Homeland Security at The George Washington University. Prior to his current work as a security consultant, Clint served as a U.S. Army infantry officer, a FBI Special Agent on a Joint Terrorism Task Force, and as the Executive Officer of the Combating Terrorism Center at West Point.

J.M. Berger is an author and analyst studying extremism and the use of propaganda on social media.

Image: Andrew E. Weber