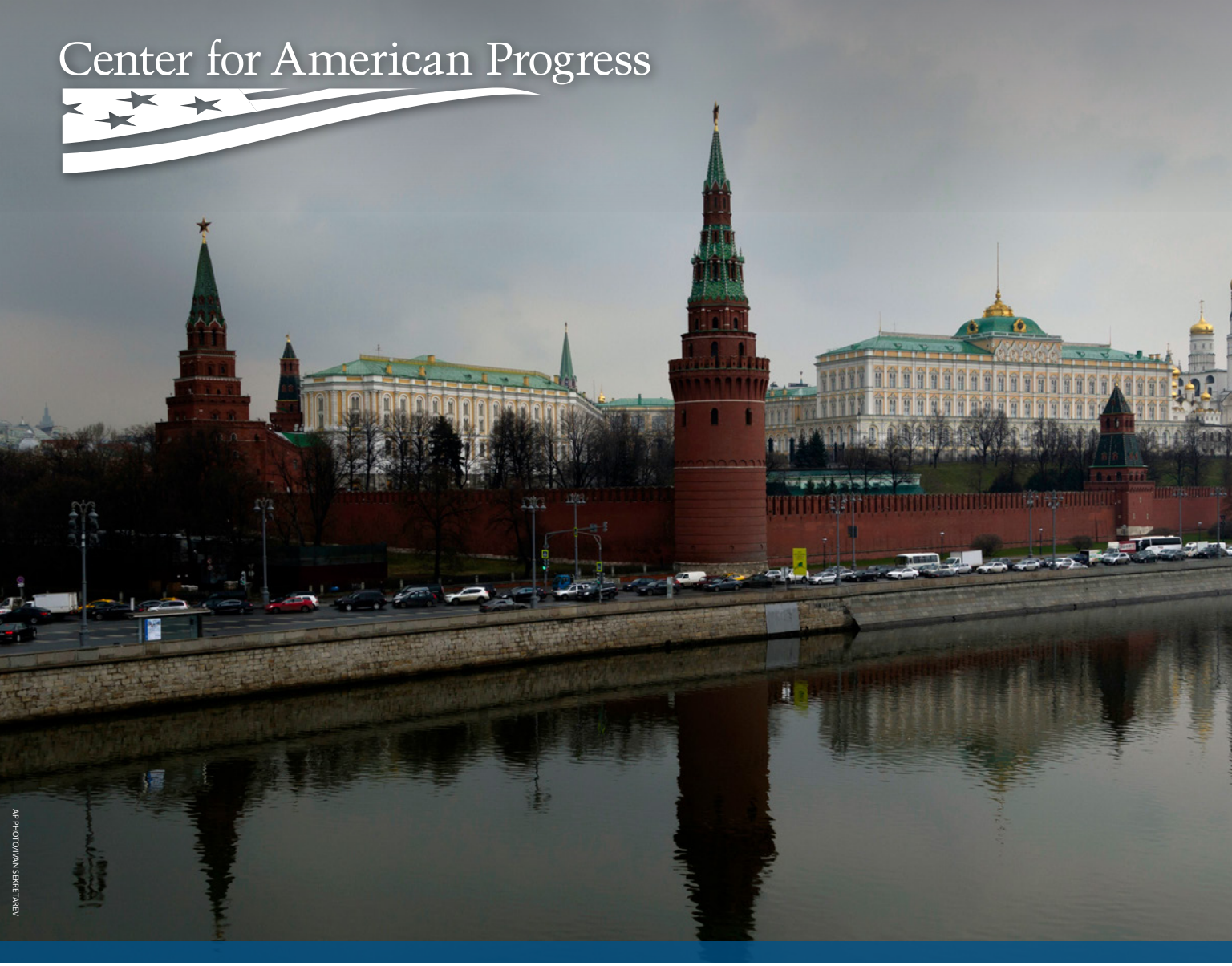
Center for American Progress



AP PHOTO/IVAN SEKRETAREV

War by Other Means

Russian Active Measures and the Weaponization of Information

By Max Bergmann and Carolyn Kenney June 2017

Center for American Progress

War by Other Means

Russian Active Measures and the Weaponization of Information

By Max Bergmann and Carolyn Kenney June 2017

Contents

Introduction and summary

Liberal democracies across the globe are under attack. They are being attacked not by traditional weapons of war but by disinformation—intentionally false or misleading information designed to deceive targeted audiences. While these attacks may not pose a threat to the physical safety of democratic citizens, they do pose a threat to democracy.

In modern democratic societies, credible information is critical to the economy, political system, and way of life that citizens have come to expect. When citizens of democracies do not trust information, the forums for discussing politics and debating policy are compromised. If the media in a democracy is viewed as biased or, worse, as aligned with special interests, the bedrock of the democratic system—its ability to resolve differences through debate, persuasion, and compromise—breaks down. A democratic society can withstand deep disagreements, but if its citizens cannot agree on some basic and fundamental facts, that democracy will struggle to function.

In 2016, the Russian Federation, under the direction of President Vladimir Putin, interfered in the U.S. election and in doing so also attacked the integrity of the American democratic system.

Russia is exploiting the openness of liberal democracies to undermine them from the inside by conducting an active measures, or aktivniye meropriyatiya, campaign that is, in effect, political warfare. These campaigns actively seek to influence the targeted society, and they involve a number of lines of effort: espionage operations to acquire information, such as through cyberhacking; information operations to disseminate disinformation, as well as spread and amplify information that advances a particular narrative; and propaganda campaigns using traditional media platforms. While these efforts are rooted in old Soviet tactics, the new online information environment makes these current efforts a qualitatively different threat than those of the past.

By taking a close look at Russian disinformation efforts, the authors of this report made the following key findings:

- The post-Cold War strategy of seeking to integrate Russia into the liberal global order is no longer operable. The United States must reset its posture toward Russia to recognize that it now confronts a global ideological competition not seen since the Cold War.

- For the Kremlin, this renewed geopolitical competition is at its core an ideological and political contest. Moscow's goal is to discredit democratic governance and the existing liberal international system.

- The new media and online environment creates enhanced opportunities for Russian active measures.

- Russia has invested heavily in developing its disinformation capabilities, effectively treating these tools as a new weapon system that it can readily use against liberal democratic societies.

- Russian information operations are integrated whole-of-Kremlin efforts that use Russia's immense intelligence and espionage capabilities, criminal networks of cyberhackers, official Russian media networks, and social media users or trolls paid by Kremlin-linked oligarchs.

- Russian media outlets such as RT—formerly Russia Today—and Sputnik, as well as websites such as WikiLeaks, serve as information launderers, playing a role similar to that of money launderers but for information.

- Russian influence efforts, including disinformation, are heavily enmeshed with U.S. alternative media.

To better understand Russia's influence operations and use of disinformation, this report will examine the history of such operations, the motivations behind them, what techniques are being used and how, and what the United States and others should be doing to respond to such actions.

How we got here

Russian active measures, specifically the use of disinformation, or dezinformatsiya, attempt to undermine public trust in the authenticity of information crucial to a healthy and lively democratic society. Russia uses disinformation in sophisticated and complex information operations that use multiple and mutually reinforcing lines of effort—through cyberhacking, the employment of cyber trolls, and overt propaganda outlets. Today's online media environment is rich with increasing political polarization, growing distrust of traditional media sources, the hardening of echo chambers, online dialogue that is caustic in nature, and the ability to spread information easily—true or otherwise—through the body politic. These factors make U.S. political discourse a ripe target for disinformation efforts. Notably, this is not a media environment or online culture that Russia created, but it is an environment that Russia has aggressively sought to exploit. The disaggregated news and social media landscape has enabled Russia to intervene in elections, discredit governments, undermine public trust, and foster internal discord in ways that it could only have dreamed of during the Cold War.

These information operations are a key line of effort in Russia's continual geopolitical competition with the United States and its liberal democratic allies.[1] Following the end of the Cold War, U.S. and European strategy toward Russia focused on integrating Russia with Europe and bringing it into the liberal global order. However, Russia remained fixed in a realist balance-of-power outlook and saw eastward expansion of NATO and the European Union not as a pathway to Russia's eventual inclusion but instead as Western encroachment and a geopolitical threat.[2] As Eastern European states joined NATO and the European Union and as the liberal color revolutions swept through former states of the Soviet Union—the Rose Revolution in Georgia, the Orange Revolution in Ukraine, and the Tulip Revolution in Kyrgyzstan—President Vladimir Putin saw these events as a potentially mortal threat to his rule and as undermining Russian influence in its near abroad—the new republics that emerged from the breakup of the Soviet Union. In the eyes of the Kremlin, the liberal color revolutions were American plots fostered through U.S. democracy promotion programs.[3] In a speech to the

Russian Ministry of the Interior in March 2015, Putin said that the West was "using so-called color technologies, from organizing illegal street protests to open propaganda of hatred in social networks" to foster revolution.[4] From the Kremlin's point of view, it faced a twin threat of NATO and EU encroachment from the outside and a potential liberal uprising from within.

The Kremlin saw these two threats converge with the Maidan Revolution in Ukraine in 2014. Protestors in Kyiv, braving the cold Ukrainian winter, occupied Maidan Square for months demanding that their corrupt government turn toward Brussels and sign an association agreement with the free and democratic European Union, a move that meant turning away from Moscow and its offer of an autocratic Eurasian Union.[5] After Viktor Yanukovych, the Kremlin-backed president of Ukraine, fled Kyiv, ceding power to the Maidan protestors, the Kremlin responded. Russia illegally seized the Ukrainian region of Crimea and instigated an insurgency in Ukraine's eastern Donbass region that continues to this day.[6]

The situation in Ukraine also led to a clear break in relations with the West. The United States and the European Union put in place sanctions against Russia and evicted Russia from the G-8. Additionally, the United States froze lower-level diplomatic contact and greatly expanded U.S. security assistance and military deployments to Europe.[7] This new geopolitical environment has led many analysts to note that the United States and Russia have entered a new Cold War.[8] However, while the events in Kyiv led to a freeze in relations, the approaches of the United States and Europe were also designed to facilitate an eventual thaw. For instance, sanctions were designed to be temporary and would end if there was progress in the Minsk negotiations over eastern Ukraine.[9] However, Moscow saw relations with the West after Ukraine not as frozen but as broken. For the Kremlin, if the allure of Western liberal democracy as embodied by the European Union was such that Russia could "lose" Ukraine—a place so valued by Putin and Russian nationalists that they sometimes refer to it as Novorossiya, or "New Russia," a reference to the czarist Russian empire—it meant that liberal democracy itself posed an acute geopolitical threat to the Kremlin.[10] A threat that, in Putin's mind, had to be matched.

As stated above, this geopolitical competition is at its core an ideological and political contest for the Kremlin. Moscow's goal is to discredit democratic governance and the international system, as well as "globalism"—shorthand for the embrace of open markets, limited borders, international institutions, and cultural liberalism and multiculturalism.[11] Today, disinformation campaigns are but one of the tools that Russia deploys to undercut democracy, especially in Eastern

Europe, within the European Union, and along Russia's periphery. Russia is also using its economic clout, including its network of oligarchs, to gain leverage in eastern Europe—and in the case of the latter, effectively using corruption as a political tool.[12] Russia has also funded far-left and far-right political parties and set up pro-Kremlin front organizations to advance pro-Kremlin narratives and polices.[13] The Kremlin is seeking to discredit and disparage liberal democratic governance both to undercut the allure of democracy to its own citizens and to weaken democratic rule from the inside.

In effect, Russia has reverted to a counterrevolutionary foreign and military policy that harkens back to the Russian foreign policy of the 19th century. In the past, Russia-led efforts were crucial to countering liberal movements and protecting traditional Europe: from defeating Napoleon and marching on Paris; to Russia's participation in the Holy Alliance of states that put down liberal advances in Italy, Portugal, Greece, and Spain in the 1820s; to the 1848 revolution in Hungary where Russian forces came to the aid of the Habsburg monarchy.[14] Soviet strategy during the Cold War was similarly focused on countering liberalism and its appeal, especially in Warsaw Pact Eastern Europe.

The re-emergence of this ideological challenge has caught the United States and Europe off guard. While the United States has scaled back its public diplomacy and democracy promotion efforts, Russia is treating the information domain like a new theater for conflict and has invested in developing its capabilities just as it would in developing a new weapon system. As senior Kremlin adviser Andrey Krutskikh summarized at a Russian information security forum in January 2016:

> *You think we are living in 2016. No, we are living in 1948. And do you know why? Because in 1949, the Soviet Union had its first atomic bomb test. And if until that moment, the Soviet Union was trying to reach agreement with [President Harry] Truman to ban nuclear weapons, and the Americans were not taking us seriously, in 1949 everything changed and they started talking to us on an equal footing. … I'm warning you: We are at the verge of having "something" in the information arena, which will allow us to talk to the Americans as equals.*[15]

Krutskikh's comments are reflective of how the Kremlin sees information operations—a domain where Moscow has the advantage and where it can level the power dynamic between Russia and the United States and Europe. More than a year after Krutskikh made those comments, it is abundantly clear what he meant. The United States and Europe now face an ideological competition not seen since the Cold War.

The dezinformatsiya weapon

The deployment of disinformation has long been part of Soviet and Russian military strategy. During the Cold War, the Soviet Union saw the West's open media environment as an ideal space to undermine confidence in Western government institutions and the West's governing model.[16] Ivan Agayants, a general for the KGB—the former Russian secret police and intelligence agency—who political scientist Thomas Rid describes as "the KGB's grandmaster of *dezinformatsiya*," commented in 1965 that "if they [the West] did not have press freedom, we would have to invent it for them."[17]

Soviet intelligence sought to amplify failings within the United States, such as in the area of civil rights, and pushed fake stories and conspiracy theories to discredit the West, including the claim that the CIA was responsible for inventing AIDs.[18] According to Rid, by the 1960s, "disinformation—or active measures—were well-resourced and nearly on par with [intelligence] collection in the KGB … The Cold War saw more than 10,000 individual Soviet bloc disinformation operations."[19] While Soviet dezinformatsiya efforts were vast, the relative concentration of the news media and the slower pace of the news cycle limited its effectiveness. The information and communication revolution of the past two decades, however, has transformed the information domain and created new access points for the Kremlin to conduct disinformation operations.

Putin was slow to recognize the disruptive power of the internet, focusing his energy after coming to power in 2000 on exerting control over Russian television and newspapers. However, the role social media played in helping organize protests in Moscow and St. Petersburg in 2011 and 2012 led to a change in the Kremlin's approach.[20] As the Kremlin woke to the disruptive power of the internet and social media, it sought to exert control and worked to develop its capacity to disrupt the ability of opponents of the Kremlin to organize and communicate online. *Time* reported that after being re-elected in 2012, "Putin dispatched his newly installed head of military intelligence, Igor Sergun, to begin repurposing cyberweapons previously used for psychological operations in war zones for use in electioneering."[21] A report from the Institute of Modern Russia explains:

If at the advent of the Internet age, online activity was seen as essentially politically liberating, a censorship-busting tool that would undermine authoritarian regimes, it is quickly turning into a weapon for postmodern dictatorships like the Kremlin's, which rely more on manipulating societies from inside than on direct oppression. The underlying mindset … [is] the idea that "truth" is a lost cause and that reality is essentially malleable.[22]

As the Kremlin disrupted its domestic opposition online, it also learned tactics, techniques, and procedures that it would use to inform its disinformation operations against Europe and the United States.

In recent years, information operations have become an ever more important part of Russian military strategy. In 2013, the chief of the general staff of the Russian army, Valery Gerasimov, stated as much when he said that the use of nonmilitary tools such as disinformation had become as important if not more important than more traditional military means.[23] Following the Maidan Revolution in Ukraine, Russia followed a hybrid warfare doctrine, in which information operations played a critical role. Russia used "little green men"—Russian forces without insignia—to occupy Crimea and instigate an uprising in eastern Ukraine and used information operations both to deny its involvement and to advance so-called alternative, or fake, stories to attack Ukraine and mask its military intervention.[24] When Malaysia Airlines Flight MH17 was shot down in Ukraine with advanced Russian anti-aircraft weaponry provided by the Kremlin to poorly trained Russian-backed rebels, Russia immediately went on a disinformation offensive, blaming the CIA or Ukrainian forces.[25]

A declassified U.S. intelligence community (IC) report on Russia's activities during the 2016 U.S. election concluded that "Moscow's campaign aimed at the US election reflected years of investment in its capabilities, which Moscow has honed in the former Soviet states."[26] This was underscored in February when Russian Defense Minister Sergey Shoigu acknowledged in an address to the Russian Duma that the Russian military operates a "cyber army" of 1,000 operatives at a cost of $300 million annually.[27] Commenting on Shoigu's address, Gen. Yuri Baluyevsky, the former Russian military commander-in-chief, said that success in information warfare "can be much more important than victory in a classical military conflict, because it is bloodless, yet the impact is overwhelming and can paralyze all of the enemy state's power structures."[28]

While information operations have become a key part of Russian military strategy, the tools that the Kremlin uses to conduct these operations extend well beyond its military. Russian information operations are often integrated whole-of-Kremlin efforts, using Russian intelligence and espionage capabilities, criminal networks of cyberhackers, official Russian media networks, and social media users or trolls paid by Kremlin-linked oligarchs. According to an IC assessment, Russian influence campaigns are "designed to be deniable because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations."[29] As such, these operations utilize tactics that blend covert and overt operations, creating a very complex and sophisticated disinformation system that works on multiple, mutually reinforcing levels.

Russian information operations can be broken down into three lines of effort: covert; semi-covert; and overt.[30] While distinct, each of these efforts feeds into and strengthens the others.

Covert: Spy, hack, steal, and launder

What makes Russian disinformation operations incredibly effective is that Russia uses its immense espionage capabilities in the service of its information operations.

The Russian intelligence services employ highly advanced information gathering tools—tools also used by U.S. intelligence agencies.[31] Just as the U.S. National Security Agency has the ability to monitor and capture electronic communications, so does Russia. Additionally, Russia's intelligence services—the SVR, or foreign intelligence, and the GRU, or military intelligence—are also very adept at espionage and collecting human intelligence, just like the United States' CIA or the United Kingdom's MI6. While Russia's intelligence prowess is well-known, it is the Kremlin's willingness to use information gained through intelligence means for information operations that makes these operations unique and so effective. The Russians are willing to deploy information gained through espionage in a way from which other governments have largely shied away.

Russia's interference in the U.S. election and its willingness to use espionage tools for information operations was foreshadowed by the Kremlin's 2014 release of a recording of a phone call between former U.S. Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland and former U.S. Ambassador to Ukraine Geoffrey Pyatt. The call was uploaded to YouTube. On the call, Nuland

and Pyatt discussed Ukraine's leadership transition, and Nuland, now infamously, says "f--- the EU."[32] Russia used its intelligence tools to capture the communications and then release the recording to advance its narrative that the United States was meddling in Ukraine, as well as to attempt to sow discord between the European Union and the United States. What is notable, however, is that most intelligence services would have shied away from deploying information gained from sensitive intelligence tools in such an operational way. The objective of most intelligence services is to gain intelligence to inform policymakers. By making that call public, the Russians alerted Nuland and Pyatt to the fact that their calls were being monitored and thereby burned a potentially valuable information source. Moreover, this incident also prompted other U.S. government officials to increase their vigilance about their own communications, possibly burning other Russian sources of information. In other words, releasing the call had a clear intelligence cost to Russia, yet the Kremlin released the call anyway. Moscow placed greater priority on advancing a narrative than on maintaining its access to intelligence. This is a calculation that Western intelligence agencies would almost never make.

Russia has invested in developing its cyberhacking capabilities. For instance, the Russian military's Main Intelligence Directorate, or GRU, has developed units of cyberhackers, which have been responsible for a number of high-profile hacking efforts. The GRU hacking units have been identified variously as Fancy Bear, APT28, STRONTIUM, and Operation Pawn Storm.[33] The U.S. IC found "that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures."[34] This same GRU group was also responsible for the 2015 hack of the German Bundestag, or Parliament. Hans-Georg Maassen, the head of Germany's domestic security agency, stated, "We recognize this as a campaign being directed from Russia … for disinformation or for influencing operations … Whether they do it or not is a political decision ... that I assume will be made in the Kremlin."[35] Furthermore, private cybersecurity companies have identified a clear pattern. Ed Cabrera with Trend Micro, a security software firm, said, "the victimology—when they are attacking, how they are attacking, and who they are attacking"—all align with Kremlin interests. He said these GRU-tied units push well-crafted phishing campaigns to gain access to accounts. These groups may also use a technique known as tabnabbing—essentially, spoofing a fake webmail page that says the user's log-in information is expired and to re-enter the user's credentials.[36]

One unique aspect of Russian efforts, according to a senior British intelligence official in an interview with the *Financial Times*, is that Moscow has also "fostered a network of 'modern privateers'," effectively emulating state-sanctioned piracy

of centuries ago where monarchs green lighted pirates to plunder foreign ships. Another U.S. intelligence official told the *Financial Times* that "the links between Russia's state agencies and criminal networks when it comes to aggressive cyber activities are deep and developing."[37] These criminal cyber actors are essentially allowed to operate unimpeded if they confine their efforts outside Russia and serve the needs of the Kremlin when called upon. As a result, Russia serves in effect as a safe haven for cybercrime against the West. Moreover, these private hackers also give the Kremlin additional cyber firepower and the ability to surge its efforts when needed.

The Russian hacking and subsequent release of emails from the Democratic National Committee (DNC) and from Clinton campaign chairman John Podesta represented, according to the IC, an "unprecedented" intervention in the U.S. election process.[38] The private cybersecurity firm CrowdStrike identified Russian hacking units Fancy Bear and Cozy Bear as the culprits behind the DNC and Podesta hacks, which was later corroborated by U.S. intelligence.[39] Similarly, in the French elections, a massive document dump of stolen files from the campaign of Emmanuel Macron, the eventual winner, was released in the final few days of the election. It is not uncommon for foreign intelligence agencies to penetrate political campaigns in an effort to gain insight into future policy approaches. However, Russia was not seeking intelligence; it was seeking to influence the U.S. and French elections and the democratic process in both countries.

Russia also does not seem particularly concerned about covering its tracks and may even want the victims to know that it was behind the hackings. Following the DNC hack, Michael Buratowski of Fidelis Cybersecurity commented that it was clear Russia was behind the hacking, as it used "Russian internet addresses, Russian language keyboards, and the time codes corresponding to business hours in Russia."[40] Similar "digital 'fingerprints'" pointing to Russia were found following the hacking of the Macron campaign.[41]

After hacking into and collecting emails from the DNC and Podesta, the GRU, posing as the persona of Guccifer 2.0, laundered the content through WikiLeaks. It remains unclear whether WikiLeaks serves as a witting or an unwitting accomplice used by a foreign intelligence agency. Regardless, WikiLeaks served as the vehicle for Russia to publicize the stolen information with a veneer of deniability. While WikiLeaks released and promoted thousands of stolen emails, it appears to have done so selectively and strategically, with the goal of influencing the 2016

campaign and election. For instance, many emails were never released.[42] That being the case, the information being released and publicized is not "leaks" from a concerned actor with legitimate access to sensitive information but rather stolen information laundered by a foreign intelligence service.

The timing of the email releases was also designed for political effect. The DNC emails were released right before the Democratic National Convention in an effort to drive a wedge within the Democratic Party. Podesta's emails were released just 29 minutes after the release of Donald Trump's infamous "Access Hollywood" tape, and Macron's campaign emails were released in the final days of the French election.[43]

A critical factor in the success of these operations is the complicity of the press. While WikiLeaks served as a vehicle to launder the stolen information during the American campaign, the American press, as noted by Rid during his testimony to the Senate Intelligence Committee, also effectively served as "unwitting agents" of Russia in its eagerness to report on the stolen content.[44] Here the contrast to the reaction of the French press is striking, including the fact that the main French newspaper *Le Monde* refused to write about the stolen material until after the election, while *The New York Times* and other key U.S. media gave extensive coverage to Podesta's emails and the hacked DNC material.[45]

What makes the new online information landscape so troubling is that Russia, as well as other foreign actors, has been able to greatly expand its espionage efforts against the United States with little consequence. Before the internet and social media, cultivating intelligence assets in the United States largely had to be done in person and was therefore more difficult and incredibly risky. This forced Soviet and Russian intelligence to be highly selective with their efforts. But now Russian intelligence can target Americans en masse and can do so with impunity from thousands of miles away. For instance, citing information from the cybersecurity firm SecureWorks, Rid found that in a period of 14 months, the GRU sent "19,300 malicious links, targeting around 6,730 individuals."[46] This yielded for Russia troves of information that it can deploy to influence events, attack its enemies, extract financial or business data, shape public opinion, and potentially blackmail and recruit foreign agents.

Semi-covert: Troll, forge, disrupt, and amplify

Where Russia has innovated is in its incorporation of semi-covert cyber operators into its information operations. Russia uses paid social media users, or trolls, to form an army of online cyber operators and propagandists. These operators serve as online foot soldiers engaging in keyboard-to-keyboard combat on the front lines of Russia's information war, working to elevate, disseminate, and amplify information that advances Kremlin objectives. Individually, their impact may be minimal, but collectively and operating in concert with other efforts, these operators have a strategic effect.

To build up these forces, the Kremlin has set up front organizations such as the Internet Research Agency, or the Agency, based in St. Petersburg. Funded by a Russian oligarch with ties to the Kremlin, the Agency was estimated to employ around 400 people with a budget of about $400,000 per month, with a typical employee working a 12-hour shift for approximately $700 per month.[47] In 2014, BuzzFeed reported on leaked documents regarding the Agency, finding, "On an average working day, the Russians are to post on news articles 50 times. Each blogger is to maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2,000 followers and tweet 50 times a day."[48]

These groups, known as troll farms, operate like a campaign operation. They have certain messages or themes that they are pushing or advancing for that day or a week. This action can be as basic as defending the Kremlin or pushing pro-Russian content, but it can also involve advancing conspiracy theories that cast doubt on Western governments or pushing attacks on globalism. During the 2016 campaign, a major focus was spreading messages that attacked Hillary Clinton or that cast doubt on the credibility of U.S. institutions or on the election itself—in this case, claiming the election is "rigged."[49] The American intelligence community even noted that, "Pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."[50]

But the online efforts often go much further than amplifying content or spreading vitriol. For instance, Finnish journalist Jessikka Aro, who sought to highlight Russian disinformation, was harassed viciously online and falsely accused of being

a drug dealer on alternative news websites, which posted personal photos of her online. Saara Jantunen, a researcher at the Finnish Defense Forces, explained such tactics, saying, "They fill the information space with so much abuse and conspiracy talk that even sane people start to lose their minds."[51] Aro made herself a target for dezinformatsiya and of Russia's online troll army. The result was a multidimensional attack: vitriolic online harassment; the production and posting of fake or slanderous stories; even the organization of protests outside the offices of her employer. Russia effectively made an example of Aro with the designed aim of creating a chilling effect on other journalists covering Russia.[52]

While disinformation campaigns can have specific targets, they are also simply trying to create noise online and complicate or pollute anti-Kremlin narratives, meaning that the effectiveness of a singular post matters much less than the volume of posts. As Ben Nimmo, now of the Atlantic Council, explained in 2015, Russian online propaganda "largely relies on four tactics: dismiss the critic, distort the facts, distract from the main issue and dismay the audience."[53] The Kremlin therefore accepts failure as part of the process—some disinformation ploys will not catch on—and understands that if even a few of these efforts are visibly successful, the broader effort has an impact.[54] Unlike Western public diplomacy efforts, Russian information efforts enjoy broad funding support, and since there is no focus on accuracy or avoiding unwanted international or domestic blowback, there is no detailed bureaucratic organizational chart through which these operators must work. These troll farms can thus operate rapidly and with agility.

These information operations exploit the fact that social media platforms promote or elevate content that is being talked about, shared, or trending, regardless of what that content is and who and what is causing the content to be shared. A Russian operative at a troll farm can operate a number of Twitter and Facebook accounts simultaneously by programing them to operate automatically. On Twitter, a Russian operative can use automated accounts, or bots, that can rapidly amplify content. Operators can create a network of fake bot accounts known as botnets to create a reinforcing ecosystem, creating the illusion of an online community and audience. While just a single person may be operating this ecosystem, it has the appearance of credibility due to the way that social media elevates content that is shared widely. A Russian operative can therefore amplify content and have their own bots expand the popularity of a specific tweet or post, such that it gains the attention of actual users and, potentially, the press. This amplification matters because it makes it more likely for this content to spread and spill over into Facebook feeds or Google news lists. Data scientists and digital media specialists

Jonathon Morgan and Kris Shaffer found that, "In addition to Trump support and anti-Semitic, nativist rhetoric, both bots and sockpuppet accounts were more likely to discuss Russia than normal users. The bot accounts in particular mentioned Russia four times as often as other users, and were especially interested in countering the narrative that Russia was involved in swaying the election."[55]

The use of botnets also helps embolden fringe and extremist groups by creating a faux sense of their community being larger than what it is. This makes individuals with extremist views more willing to vocalize them and encourage others. This creates a degree of normalization—suddenly, for example, posting racist statements brings followers and praise instead of scorn. Samuel Woolley of Oxford University, co-author of a report on "pro-Trump bots," explained the objective of using of bots: "The goal here is not to hack computational systems but to hack free speech and to hack public opinion."[56]

Often, these trolls, bots, and botnets push fake news stories, which are routinely produced and laundered through fake news websites. For instance, in an effort to dissuade Sweden from joining NATO, stories emerged that NATO would secretly store nuclear weapons in Sweden, that NATO could attack Russia from Sweden without Swedish approval, and that NATO soldiers could rape Swedish women with impunity. More recently, the Russians have spread rumors about German soldiers stationed in Lithuania, accusing them of rape.[57]

While pro-Russia troll farms can fabricate their own fake news, they can also manipulate the online marketplace to incentivize others to create fake news for them. Many of the fake news items seen during the election were linked back to Eastern Europe—specifically, to a town in Veles, Macedonia, where an industry emerged to write fake news stories and profit off the traffic-driven advertising revenue. While these fake news creators seem to be motivated by profit, what also seems likely is that they owe their profits in part to Russian amplification through botnets, which may have driven traffic to fake news stories, helping drive up their revenue from traffic-based advertising. Reporting has indicated that fake news on the right was more popular than fake news on the left; while progressives may like to believe that they are simply harder to fool, there were also fewer bots and other artificial traffic drivers during the election seeking to elevate fake progressive content.[58]

After receiving significant media attention in 2015, the Internet Research Agency claimed to have closed, rebranding itself instead as a pro-Kremlin media company. But Russian news organization RBC recently revealed that it was still operational.

The Moscow Times explained, "Despite its new status as a network of legitimate—if heavily biased news outlets—the 'troll agency' hasn't quite abandoned its old ways, RBC's report suggests." The report found that a popular pro-Trump, anti-Clinton Facebook group called Secure Borders,[59] which boasts 140,000 subscribers, was actually "managed from the St. Petersburg troll factory. … One of its posts published at the height of the election campaign and heavily advertised on Facebook, reached 4 million people on Facebook, was 'liked' more than 300 thousand times and shared more than 80 thousand times." Reporting on the RBC report, *The Moscow Times* says it discovered that a right-wing Twitter account called Tea Party News was managed from the same location: "All in all, RBC's sources say that at the zenith of the U.S. election campaign, the troll factory's accounts across different social media platforms would churn out as many as 50 million posts a month, with anti-Clinton messages getting the most attention."[60]

It is important to note, however, that Russia did not create the caustic online environment. The methods they have utilized are also widely used by others online, including by those on the right and the left. It is therefore hard to pinpoint the precise impact of Russia's online efforts, both on the election and on public discourse—which, of course, is largely by design. What is clear is that social media manipulation played a key role during the 2016 election. For example, an Oxford University professor, Philip Howard, described how pro-Trump bot networks began to use pro-Clinton hashtags to inject negative memes, links, and political messages into pro-Clinton circles.[61] Like a virus, they essentially co-opted the opponent's messaging and infiltrated her supporters. Using pro-Clinton hashtags such as #ImWithHer and #uniteblue, memes describing Clinton as corrupt ricocheted across both blue and red feeds. In one joint academic study on botnets, researchers found that "pro-Trump hashtags were inserted into more and more combinations of neutral and pro-Clinton hashtags, such that by the time of the election fully 81.9 percent of the highly automated content involved some pro-Trump messaging."[62]

It is difficult to determine precisely how much of this traffic was instigated or amplified by Russian operatives or was simply a campaign tactic by pro-Trump or far-right Americans. This degree of ambiguity has prompted defenders of the Kremlin to claim there is no proof. While it is difficult to disaggregate, the impact of Russian trolling efforts in influencing the election and polluting public discourse was no doubt significant. Russia, as a state actor, has resources and capabilities at its disposal that are much greater than those of individuals, groups, or political campaigns. Furthermore, the U.S. intelligence community report on

Russian interference highlighted the Internet Research Agency in its unclassified report and concluded that "Russia used trolls … as part of its influence efforts to denigrate Secretary Clinton."[63] Sen. Mark Warner (D-VA), ranking member of the Senate Select Committee on Intelligence, noted that, "there were upwards of a 1,000 paid internet trolls, working out of a facility in Russia … they can generate news down to specific areas … in Wisconsin, Michigan, Pennsylvania." This enabled them to push anti-Clinton messages.[64] Additionally, *Time* reported that U.S. intelligence officials found that "Moscow's agents bought ads on Facebook to target specific populations with propaganda." According to a senior intelligence official interviewed for the article, "'They buy the ads, where it says sponsored by—they do that just as much as anybody else does.'"[65]

Russian influence efforts were also heavily enmeshed with U.S. alternative media. A number of academic experts in social media analysis have documented the role of Russian trolls, bots, and botnets in amplifying content and in Russia's growing links to the alt-right.[66] In 2015, Nimmo explained that "the Kremlin media use Western commentators to amplify and validate Moscow's messages."[67] Russia's messaging and posturing has also demonstrated an intimacy with alt-right content, as shown by Russia's tweeting of a racist meme used by white supremacists.[68] Kate Starbird of the University of Washington found that "the structure of the alternative media ecosystem and the content that is hosted and spread there suggest the use of intentional disinformation tactics—meant to create 'muddled thinking' and a general mistrust in information."[69] These links are not surprising given Russia's well-documented backing of far-right political parties and extremist groups.[70]

However, the links between the U.S. alt-right media ecosystem and Russia may have involved more than just amplification. According to the American publishing company McClatchy, the FBI, as part of its investigation into Russian interference in the election, is examining whether far-right websites such as Breitbart and Infowars knowingly coordinated with Russian cyber operators. McClatchy reported that "operatives for Russia appear to have strategically timed the computer commands, known as 'bots,' to blitz social media with links to the pro-Trump stories … Investigators examining the bot attacks are exploring whether the far-right news operations took any actions to assist Russia's operatives."[71]

Overt: Propaganda pushers and fake news launderers

Russian media outlets such as RT and Sputnik serve to advance the Kremlin's agenda domestically and internationally and act as key players in dezinformatsiya operations. These outlets effectively serve as propaganda tools and so-called information underers, playing a role similar to that of money launderers but for information.

While news organizations compete for viewers, RT's low ratings have little impact on its funding. According to the U.S. intelligence community report, RT alone spends more than $190 million per year on the "distribution and dissemination" of its programming, though other reports have indicated that its budget has been more than $300 million per year.[72] This is a dramatic increase over its initial budget of $30 million per year in 2005. While this budget is incredibly large for a poorly rated news network, compared with a weapon system, it is a relative bargain. The lavish funding by the Russian state enables RT and Sputnik to attract mainstream talent and to create a slick, modern news platform. For instance, RT paid former national security adviser Lt. Gen. Michael Flynn to attend its 10th anniversary gala, where he sat at a table with President Putin and gave a talk.[73] RT has also hired prominent television personalities such as former CNN host Larry King, adding to its image as a mainstream network. However, RT was dramatically unmasked as the mouthpiece of the Kremlin when RT anchors Sara Firth and Liz Wahl publicly resigned out of disgust at being part of the Russian propaganda machinery.[74]

As part of their goal to advance the interests of the Kremlin, these so-called news organizations work to sow doubt and discredit the American and European democratic systems. RT, for instance, uses the tagline "Question More" to justify pushing conspiracy theories and sowing doubt in Western state institutions. Because RT does not have a domestic partisan agenda, it eagerly highlights voices on both ends of the political spectrum—as long as they are critical of Western governments. For instance, RT has hired prominent progressives such as Ed Schultz, who now works for RT, and had Green Party candidate Jill Stein seated at the same table at the RT gala as Flynn.[75] RT will give extensive coverage to events that portray America in a negative light, such as the protests in Ferguson, Missouri, as this coverage highlights America's continuing problems with racism and police brutality. RT will also give considerable coverage to anti-fracking stories, as it is in Russia's interest for America not to develop its natural gas industry, which could rival Russia's. RT and Sputnik's willingness to selectively highlight critical voices on the right and the left also adds to the credibility of these organizations on both sides of the political spectrum, which enhances the ability of RT and Sputnik to push disinformation.

The Institute of Modern Russia explained Russia's approach as combining "Soviet-era 'whataboutism' and Chekist 'active measures' with a wised-up, post-modern smirk that says everything is a sham. Where the Soviets once co-opted and repurposed concepts such as 'democracy,' 'human rights' and 'sovereignty' to mask their opposites, the Putinists use them playfully to suggest that not even the West *really* believes in them. Gitmo, Iraq, Ferguson, BP, Jobbik, Schröder—all liberalism is cant, and anyone can be bought."[76]

Key to RT and Sputnik's ability to launder information is creating a veneer of credibility. Much of the content published or broadcast may be legitimate news of the day. This makes it harder for viewers and readers to weed out stories that are either completely fabricated or pure propaganda. These outlets will take fake information, often originating online, and give it the veneer of credibility by reproducing it in RT- or Sputnik-produced stories. These stories are then reinjected into social media and advanced and promoted by troll farms and botnets.

Occasionally, the volume of attention given to a fake story will prompt legitimate mainstream media to report on it as well. One telling example of this chain of information laundering came in August 2016 with the spread of a false story about Turkish forces surrounding the U.S. airbase in Incirlik. According to cybersecurity experts Clint Watts and Andrew Weisburd, the false story started on Twitter, then migrated to RT's and Sputnik's Twitter accounts, and was then picked up and promoted in an "hours-long storm of activity from a small, vocal circle of users," many of whom were pro-Trump and pro-Russia.[77] A couple weeks later, during an interview with CNN, Paul Manafort—then campaign chair for Donald Trump—tried to call out the media for not covering the fabricated attack on the NATO base in Turkey, referring to the Incirlik base, which houses NATO troops. In trying to criticize the media's lack of coverage on an attack that never occurred, Trump and Manafort demonstrated a willingness to espouse false reporting from Russian state media.[78]

While RT will highlight stories on the left, during the 2016 election, stories on RT quickly made their way to alt-right U.S. media such as Breitbart. In one recent example, an RT commentator floated a conspiracy theory that President Barack Obama asked the British intelligence of the Government Communications Headquarters (GCHQ) to surveil the Trump campaign. Fox News commentator Judge Andrew Napolitano allegedly saw this content and repeated it on Fox, prompting Sean Spicer, White House press secretary, to repeat the allegation at a White House press briefing. In other words, disinformation spread from a Russian propaganda network to Fox News to the White House.[79]

An integrated disinformation campaign

These different disinformation tools in the covert, semi-covert, and overt space can also all work together in synchronized fashion to reinforce and amplify each other's efforts. One vivid example of this came on September 11, 2014, when the Office of Homeland Security and Emergency Preparedness for St. Mary Parish, Louisiana, received reports that there had been a chemical plant explosion in Centerville, Louisiana. News of the alleged explosion spread across Twitter, with hundreds of users documenting what appeared to be eyewitness accounts and videos of the explosion and one user even posting a screenshot of CNN's homepage reporting on the story. According to one YouTube video, the Islamic State took credit for the attack. In the end, however, the entire incident proved to be an extremely well-coordinated hoax by the Internet Research Agency, which involved not only the use of dozens of fake Twitter accounts but also the creation of clone news sites, a Wikipedia page documenting the explosion, and a fake YouTube video.[80] These complex efforts are designed to sow public distrust of the U.S. media and U.S. government institutions.

The state of play

Russian interference in the 2016 U.S. election through disinformation operations was identified by the U.S. intelligence community prior to the election. But the Obama administration was still in the beginning stages of developing a comprehensive policy response when the election occurred. After the election, the Obama administration, with little time left in office and understanding that the incoming Trump administration espoused a softer approach toward Russia, ultimately chose a more narrow, targeted response by expelling 35 Russian diplomats and officials suspected of being intelligence operatives; sanctioning two of Russia's intelligence services, as well as four top intelligence officers; and closing two waterfront estates in the United States that officials believed were being used for Russian intelligence activities.[81] This was appropriate but not nearly sufficient. More needs to be done to ensure that such foreign interference does not happen again.

Unfortunately, the Trump administration has done nothing to respond to the Russian attack on the U.S. democratic process. In fact, the Trump administration has signaled a willingness to ignore the attack. There appears to be no policy process underway within the Trump administration to better position the United States to deter, counter, and respond to these infringements in the years ahead.

Meanwhile, the Republican Congress, apart from a few members, has been largely muted and has instead worked to protect the White House by blocking a more thorough investigation into what happened.[82] This is incredibly shortsighted. While the Russians sought to elect Donald Trump in this election to the benefit of the Republican Party, there is no reason to believe that Russia, or another country, will not use this model again to intervene in future elections to the detriment of the GOP.[83]

Alas, Russian interference continues unabated in the politics and elections of the United States' close allies. For instance, in France, Russia hacked and released stolen campaign information from Emmanuel Macron. Former French President François Hollande has denounced Russia's attempts to "influence

public opinion," and French Foreign Minister Jean-Marc Ayrault has accused Russia of hacking activity in the country, where the Kremlin has also helped finance the far-right party led by Marine Le Pen.[84] The head of the Dutch General Intelligence and Security Service, Rob Bertholee, recently revealed that Russian intelligence hacking groups had attempted to hack the email accounts of Dutch government employees.[85] Dutch intelligence also recently determined that Russia used disinformation tools to interfere in April's referendum vote on a trade agreement between the European Union and Ukraine.[86] German intelligence also believes that the Russians hacked the emails of members of the German Bundestag—the Parliament—and their staffs, and it fears that the Russians are preparing to selectively use that hacked content to interfere in the upcoming German elections.[87] The *Financial Times* reports that according to an official at NATO, cyberattacks on the alliance are up 60 percent in the past year. Additionally, a senior security source at the European Commission noted that attacks against EU institutions are up 20 percent.[88]

Furthermore, Russian disinformation is still affecting U.S. politics, as the RT-Fox News-Sean Spicer-GCHQ affair demonstrates. According to an IC assessment, "Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes."[89]

Recommendations: What the United States should do in response

The post-Cold War strategy of seeking to integrate Russia into the liberal global order is no longer operable. Russia under Vladimir Putin will continue to position itself as a geopolitical adversary of the United States. The United States needs to reset its posture toward Russia to recognize that it now confronts a global ideological competition not seen since the Cold War. The ideological challenge that communism posed to liberal democracy has been replaced by authoritarian nationalism.

While disinformation operations are a key Russian tool in this ideological contest, they are ultimately an asymmetric tool used by a weaker power to level the playing field. Russia lacks the economic and military capacity to challenge the United States and its allies directly, and strongman-authoritarian governance lacks the ideological pull of liberal democracy. A key facet of responding to an adversary using an asymmetric tool is not to respond in a way that undercuts one's own strengths. Countering disinformation is not about fighting fire with fire. The United States should not conduct disinformation campaigns, as doing so would only play into the hands of the Kremlin by adding to the cognitive dissonance that undercuts democracy and would be relatively ineffective against relatively closed societies.

Instead, the United States must seek to improve efforts to deter, detect, and counter disinformation. The United States must also recognize that countering disinformation and defending the truth means playing defense. Therefore, the United States needs to look to other tools through which it can go on the offensive, impose costs, and deter future attacks. Countering Russian disinformation requires playing offense and defense and should be embedded within a broader strategy toward challenging Russia in this new ideological contest, especially by standing up strongly in defense of democracy and human rights. It should be noted that effectively countering Russian disinformation will require vastly more commitment on the part of the U.S. government, especially as it is currently headed by a president who, along with his surrogates, has actively pushed disinformation.

To effectively respond to the Russian threat to democracy, the United States should:

Immediately impose meaningful costs on Russia to deter future attacks against the United States and its allies

While an outgoing administration could only do so much, evicting diplomats and intelligence agents, as the Obama administration did on December 29, was not enough. Russia benefits economically from its access to open liberal societies, while at the same time it uses its access to undermine them. Congress should impose robust sanctions that further isolate Russia's economy and starve its oligarchs of their easy access to launder money into the West.[90] The United States must also send a message to other countries that if they intervene in the U.S. democratic process or that of its allies, the costs will be severe. Unfortunately, while there seems to be bipartisan support for stronger sanctions in Congress, the Republican leadership, including Chairman of the Senate Foreign Relations Committee Sen. Bob Corker (R-TN), are blocking action.[91] As a result, the administration and the congressional majority are leaving the United States and its allies in Europe dangerously exposed. Putting in place stronger economic sanctions is a necessary first step in establishing a modicum of deterrence, since more in-depth policy responses will take time to put in place.

Establish an independent commission to conduct a top-to-bottom assessment of the U.S. government's tools and capabilities to counter the Russian threat

The U.S. government is simply not positioned to respond effectively to foreign information operations. As former FBI Special Agent and cyber and homeland security analyst Clint Watts noted in his testimony to the Senate Intelligence Committee, the U.S. national security bureaucracy has become heavily tilted toward counterterrorism efforts over the past 15 years.[92] While these efforts are vital, it is clear that more attention and resources need to be allocated to countering the threat from foreign information operations. Following the attacks of September 11, an independent 9/11 Commission was set up and proved crucial not just to getting to the bottom of what happened but also to providing recommendations for how the U.S. national security bureaucracy should reform itself to counter the terrorist threat. The United States needs an independent commission modeled on the 9/11 Commission to conduct a top-to-bottom examination of

the U.S. national security bureaucracy to identify new approaches, reforms, and actions necessary to confront the threat of foreign information operations. This should involve a thorough review of U.S. cyber, intelligence, homeland security, law enforcement, diplomatic, and public diplomacy tools and provide recommendations to better posture the United States to tackle this threat.

- **The U.S. Department of Homeland Security and state governments need to take urgent steps to protect the integrity of our voting systems.** While the Department of Homeland Security and the intelligence community determined that Russia did not alter vote tallies in the 2016 election, they did conclude that Russia had gained access into the systems of some state voter registration systems.[93] This represents a clear and present danger to the integrity of elections. While Russia may not have manipulated voter tallies this time, there is no guarantee that it—or another actor—will not do so next time. As former Assistant Attorney General for National Security John Carlin argues, voting systems should be seen as "critical infrastructure," and the United States should have a "nonpartisan warning system" going into the next election if there are indications of hacking efforts.[94]

- **Give greater priority and resources to combating cyberhacking and intrusions, especially those related to elections.** The Obama administration significantly expanded the government's attention to cyberhacking. However, the lackadaisical FBI response to the Russian hacking of the Democratic National Committee is unacceptable and demonstrates that greater vigilance is needed, especially relating to elections and political campaigns. The government should be ready and able to respond rapidly when there are potential state-sponsored hacking attempts on political parties, candidates, and election-related offices.

- **Political campaigns must also take stronger steps to protect and defend themselves.** Beyond simply taking cybersecurity seriously and adopting smart and thorough cybersecurity procedures, campaigns should look to some of the steps taken by the Macron campaign in France. Well aware that it was a target for Russian espionage, the Marcon campaign went on a counteroffensive against the hackers to sow confusion and waste their time. The campaign claimed to have planted fake documents, signed on to phishing emails, and flooded the hackers with fake passwords and logins.[95] This enabled the campaign to highlight that some of the files that were dumped online were fake, which complicates the media's ability to report on the information.

- **U.S. Cyber Command and the intelligence agencies need to assess their cyber tools in light of the Russian cyber operations.** What seems evident from the Obama administration's policy response is that U.S. cyber tools, while likely the most powerful in the world, are not nearly as nimble, creative, or flexible as believed. In light of the 2016 attack, the United States needs to assess whether it is prioritizing the right operational objectives and is appropriately postured to counter disinformation campaigns in the cyber realm. Actions should include going after Russian hackers or exposing Russian censorship tools, as suggested by retired Admiral James Stavridis, former NATO supreme allied commander.[96] There may not be as much to be done in this space as it seems, as countering Russian actions in cyberspace with cyber tools may not be effective. The possible costs of the development of international cyber norms and the potential escalatory nature of an overt cyber response may outweigh the potential gains of such a response. But given the threat posed by Russian information operations, it is necessary to assess whether U.S. cyber resources are being deployed effectively and whether the United States is making the investments needed to develop the right capabilities in light of Russian efforts. For instance, Hans-Georg Maassen, the head of Germany's domestic security agency, expressed the need for Germany to develop offensive cyber capabilities: "We believe it is necessary that we are in a position to be able to wipe out these servers if the providers and the owners of the servers are not ready to ensure that they are not used to carry out attacks."[97] The United States should similarly explore using its cyber tools to destroy stolen information before it can be deployed for disinformation campaigns.

- **Structure intelligence disclosure policies and practices to give greater priority to countering disinformation and advancing public diplomacy goals.** The United States could potentially use its intelligence tools to counter disinformation in a more effective manner and in so doing advance public diplomacy goals. In general, the United States is extremely reluctant to make intelligence information public to advance public diplomacy policy goals. This reluctance is sensible, but it can also severely limit the United States' ability to make its case to a foreign government or public or to push back on incorrect information. For instance, U.S. diplomats are often put in the position of pressing countries to take action on nonproliferation cases—such as providing warnings to a country to stop and search a cargo ship in its port carrying illicit nuclear materials—but cannot fully disclose the information in order to protect intelligence sources and methods. This often leaves the United States in a "trust us" mode—a posture that can hinder the ability to convince countries to take action. In the case of

information operations, this means that even if the United States has information that could advance U.S. public diplomacy objectives vis-à-vis Russia or could be effective in countering Russian disinformation or in embarrassing the Kremlin—information akin to Russian kompromat, such as knowledge that a senior leader has a mistress or evidence of corruption—that information is rarely injected into the public domain. Admittedly, this is a difficult balance to strike, but in weighing intelligence disclosure decisions, it is likely that greater weight should be given to the policy objectives of countering disinformation and advancing U.S. public diplomacy. After all, the intelligence community should serve broader U.S. policy objectives.

- **Expand counterintelligence efforts.** The United States needs to up its intelligence and counterintelligence efforts concerning Russia. Since 9/11, counterterrorism has appropriately been the priority. However, given the escalation of Russian influence and espionage efforts, more resources and personnel need to be devoted to countering Russian espionage within the United States.

- **Push at a high level to strengthen international cyber norms.** Developing the rules of the road in cyberspace is immensely challenging. Given the difficulties of assessing attribution, the prevalence of nonstate actors, and the difficulty in determining the line between what constitutes a cybercrime or traditional espionage and what constitutes a cyberattack, which is an act of war, is extremely unclear. These issues complicate efforts to emulate nuclear arms control efforts. Nevertheless, the fact that cyberspace represents a unique challenge does not mean that efforts should not be pursued to establish and reinforce norms, develop codes of conduct, or reach an arms-control style treaty. Rep. Jim Himes (D-CT) has similarly pointed to the need to negotiate a treaty to lay out international standards of behavior in cyberspace, just as the Geneva Conventions did for conventional warfare.[98]

  Progress has been made. In 2015, following bilateral discussions between the United States and China, the G-20 affirmed in a statement that no country should "conduct or support cyber-enabled theft of intellectual property" with the goal of gaining a competitive economic advantage.[99] In an effort to advance international cyber norms, the U.S. Department of State has sought to affirm the applicability of existing international law to the cyber domain, forge norms relating to state behavior during peacetime, and build confidence to foster cooperation among nations. But for ongoing U.S. efforts to gain momentum, high-level

effort is needed. In 2010, for instance, President Obama held a nuclear security summit, which put a spotlight on loose nuclear material and helped prompt international action.[100] A similar high-level effort is needed to elevate this issue on the international agenda and prompt international action.

- **Establish boundaries and deterrence in cyberspace through the clear messaging of U.S. cyber redlines and by loudly calling out cyber intrusions.** Developing clear messages and redlines about what the United States would deem to be a cyberattack under the law of war could decrease ambiguity and help deter such attacks against America. Indeed, President Obama privately confronted President Putin at the G-20 summit in China and warned him that hacking the voting systems would cross the line and merit a strong retaliatory response.[101] The United States should more clearly articulate sectors that it believes should be off limits to a cyberattack and warn that if these sectors are deemed to be under attack—such as interference in an election or an attack on critical infrastructure—the United States will respond forcefully.

Develop tools to shine a spotlight on disinformation to build public resilience

Ultimately, efforts to expose disinformation are about playing defense. These efforts will inevitably manifest as a reaction to events, rather than shaping those events. As a result, a response is likely to be slower and more bureaucratically cumbersome than the more agile Russian disinformation bureaucracy, which is not worried about accuracy. Nonetheless, improving U.S. defenses is critical, and when it comes to disinformation, sunshine can be a great disinfectant. U.S. efforts should not focus on debunking every falsehood online but instead on raising public awareness and resilience. The Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), which primarily focuses on cybersecurity and serves as an important liaison with the private sector, should have its mission expanded. It should be given the resources and capabilities to publicly expose foreign operatives online and to debunk fake news relating to U.S. government activities. US-CERT should also work closely with the State Department's Global Engagement Center, which has a similar mission abroad. This expanded mission for US-CERT could involve efforts to:

- **Detect and monitor.** Identifying and monitoring foreign information operations will require additional resources and the hiring additional of personnel. As Clint Watts explained in his testimony to the Senate Select Committee on Intelligence, the intelligence agencies have not prioritized unclassified open source information.[102] The United States needs to expand its efforts to monitor and track foreign actors operating in cyberspace.

- **Notify and highlight.** Once the United States is better able to detect information operations, it should do more to notify the public and news media of the current environment. Many Nordic and Baltic states are much more resilient to Russian disinformation efforts, as their publics have become familiar with Russian actions and tactics. Russian disinformation efforts have been identified and highlighted by the political leadership of these states; as a result, their press members have become more skilled at detecting these campaigns. Following suit, U.S. government officials should do more to notify and brief the public and press on foreign information operations.

- **Debunk misinformation.** The United States could also emulate the European Union's efforts to counter Russian disinformation by publicly identifying and highlighting fake information. In 2015, the European Union established a disinformation task force dubbed East StratCom to address Russian disinformation campaigns. The task force scours the internet for fake news and disinformation, highlighting disinformation efforts on its Twitter account and sending it out in biweekly newsletters called the Disinformation Review.[103] For instance, following the April terrorist attack in Stockholm, the Disinformation Review highlighted how pro-Kremlin outlets spread conspiracy theories and manipulated photos after the tragedy, noting that this fit a familiar pattern.[104] As of November 2016, the newsletter had 20,000 readers each week,[105] with a major audience for the material being journalists who can use it as a resource to avoid being duped.

- **Troll the trolls.** Just as the United States monitors social media for counterterrorism purposes, it could develop its ability to detect state-sponsored operators. The United States could alert American users who interact with these operatives, or their controlled bots, that the accounts they are interacting with are either suspected agents of a foreign government or are bots controlled by suspected agents. A U.S. government account, operated by US-CERT, could effectively troll the trolls by pointing them out and shining a spotlight on their efforts. This sort of interaction would be similar to Google's warning to Gmail users that a

state-sponsored entity is seeking to hack someone's email.[106] Establishing this capacity would require additional resources and manpower but could likely rely on the same type of automation used by Kremlin-controlled bots.

- **Name and shame.** The United States should more aggressively name and shame countries that violate norms of cyberspace. The Obama administration's more aggressive approach to China in the cyber domain, for instance, prompted China to come to the table.[107] While it is unlikely that naming and shaming would have a significant impact on Russia, it would help highlight its behavior for the public and would make Russian information operations a major bilateral irritant, forcing it on to the bilateral agenda. It would also prompt the rest of the international community to take notice and can serve to isolate.

Significantly expand public diplomacy efforts

Efforts to counter disinformation are defensive and reactive in nature. But the United States can go on the offensive in the information space by significantly expanding its public diplomacy efforts. In testimony to the Senate in January, James Clapper, then-director of national intelligence, said that America needs a "USIA [U.S. Information Agency] on steroids," as we need "to fight this information war a lot more aggressively."[108] While an independent commission should assess recreating the USIA, as a first step Congress should increase funding for the existing, though severely underfunded and neglected, public diplomacy tools.

As the United States cut funding for public diplomacy efforts after the Cold War, Russia—as well as countries such as Iran and China—significantly expanded funding of state-supported media.[109] Meanwhile, many Western news networks decided it was not profitable enough to invest in foreign language media in small markets in places such as the Balkans. Russia has sought to fill this gap in the news media marketplace through the expansion of Russian-state funded media. Many of the local media environments are increasingly Russian-dominated—where anti-U.S., anti-NATO, anti-EU, and anti-democratic messages carry the day.[110]

Yet despite the urgent need for increased U.S. efforts, the Trump administration is proposing massively cutting funding for the State Department and, as a consequence, cutting efforts to counter Russian propaganda. Specifically, President Trump's fiscal year 2018 budget calls for a 31 percent cut in funds to the State Department and the U.S. Agency for International Development, which, if

enacted, would reduce spending as a percentage of U.S. gross domestic product to its lowest levels since World War II.[111] While Trump's budget was light on details, these cuts would seriously affect critical diplomacy programs aimed at countering attacks on the United States and its allies. This is exactly the wrong approach.

The United States needs to support and expand efforts to provide an independent alternative to Russian disinformation. Doing so requires significant expansion in funding efforts for U.S.-sponsored outlets such as Radio Free Europe/Radio Liberty and Voice of America, which are funded by the United States but governed by the Broadcasting Board of Governors; therefore, the U.S. government has no operational or editorial input. Like the Public Broadcasting Service (PBS) and National Public Radio (NPR) here in the United States, these outlets serve as a source of independent news and as the surrogate free press where the press is stifled, producing content in more than 25 languages. Radio Free Europe/Radio Liberty and Voice of America also launched "Current Time" earlier this year, a fact-based Russian language 24-hour news channel designed to provide a fact-based alternative for Russian speakers.[112] These efforts, however, remain woefully underfunded and fall short of what is needed to challenge Russian-backed media, which has become entrenched in many countries.

As part of this investment, the State Department should also revamp its approach to public diplomacy. The National Defense Authorization Act for Fiscal Year 2017 (NDAA), expanded the mandate of the Global Engagement Center (GEC) beyond countering the Islamic State messaging to countering disinformation from state actors. The NDAA also authorized a significant increase in the GEC budget from $5 million to up to $80 million.[113] Secretary of State Rex Tillerson should implement the changes authorized in the NDAA and prioritize the expansion of the GEC, including expanding its collaboration with NATO and the European Union. Additionally, the State Department's Bureau of Public Affairs Rapid Response Unit, which monitors foreign news and reports trends, should feed its efforts into the GEC.[114]

In addition, the State Department should prioritize public diplomacy tours and trainings for its foreign service officers, and Congress should support education and cultural exchanges that are supported by the State Department's Bureau of Educational and Cultural Affairs. The State Department should also take steps to end a climate of caution prevalent among public diplomacy officers, who fear being punished if their engagement with the public ever goes awry. For example, Senior Public Affairs Officer Larry Schwartz, in Egypt, was recalled from Cairo

back to Washington because of a tweet directed at an Egyptian audience with which some on the U.S. far right took issue.[115] His recall to Washington sent a chilling effect throughout the State Department—engaging the public could put your career at risk. The State Department and the U.S. government need to develop a thicker skin if public diplomacy efforts are to be effective.

Social media companies should take steps to avoid being unwitting agents

The erosion of trust in online content and information could have far-reaching economic impacts. The emergence of a new "sharing" economy is built on public trust of online tools. It took years for the public to gain trust in online venues, as the public was dubious of online interactions in the early years of the internet. If consumers no longer trust the information they are receiving on social media sites and fear sharing financial information or conducting online transactions due to threats from hacking, this will have a far-reaching impact on Silicon Valley. Social media companies need to do more to address the fact that their platforms are being used by foreign governments as vehicles to conduct information operations.

Since the election, Facebook and Google have taken some steps to tackle this issue. In fact, Facebook recently released a report acknowledging that bad actors, including governments, have exploited the platform to "manipulate civic discourse and deceive people." In the report, Facebook claims that it has developed "new analytical techniques" specifically "to uncover and disrupt" such abuse on its platform, which in the case of France, recently enabled Facebook to take action against 30,000 fake accounts.[116] Facebook has also started to implement a third-party fact-checking tool to combat fake news that warns users when content is disputed.[117] Additionally, Facebook has taken steps to change the algorithm for its trending section, which will now try to promote topics that are not only popular but also have multiple related articles to try to prevent viral false stories from being listed.[118] Meanwhile, Google has announced the expansion of its use of fact-checking tags, whereby news search results are tagged with such phrases as "mostly true" or "false" if stories have been checked. Google has paired up with more than 100 news and fact-checking organizations whose conclusions appear in search results if they have met certain criteria.[119] Both Facebook and Google have also taken actions against fake news sites directly, with Google banning websites

that spread misinformation from using its online advertising service and Facebook clarifying its ad placement policies to include not displaying ads for sites that include fake news.[120] Google reported that as a result of this change, it had banned 200 publishers from its advertising network.[121]

In a *Daily Beast* article, Clint Watts and Andrew Weisburd recommend that social media companies fund the creation of an independent news rating system akin to Consumer Reports.[122] This rating agency would create a system for rating the accuracy of the source of the information, as opposed to assessing the content of the information. Watts compares it to providing nutrition labels on food products, which gives consumers the information to make informed judgments about what they eat but does not stop consumers from eating fatty food. Similarly, a rating system on news would provide social media users with information about the news they see but would not block this news from being shared or violate anyone's freedom to consume the fake news. As Watts and Weisburd note, "If social media users choose to read junk news and be mind fat, they have no one to blame but themselves."

Notably absent from the list of giant tech companies trying to tackle this issue is Twitter, which is problematic given that a recent study found that up to 15 percent of Twitter accounts are run by bots, not people, which translates to nearly 48 million bot accounts on the platform.[123]

However, some outside groups have developed tools for users to track disinformation themselves. For instance, Indiana University and the Center for Complex Networks and Systems Research have created a new tool called Hoaxy that allows users to conduct searches to track the origins of claims and how they spread on Twitter and to analyze the information available to determine for themselves whether a claim or rebuttal is true.[124] Researchers at Indiana University previously developed a tool that helps identify whether a Twitter account is being operated by a bot.[125]

There is, however, still considerable doubt that these steps are sufficient to address the problem of the spread of disinformation on these platforms. Social media companies may be reluctant to crack down on bots and other artificial users because these accounts and the traffic they generate increase companies' user statistics, making their platforms seem more widely used—and therefore more valuable, which increases share price. This is manipulation, and advertisers on Twitter are beginning to notice.[126]

News media must avoid being unwitting agents

The news media is critical to building social resilience to disinformation. The press needs to assess its journalistic standards when it comes to its approach to stolen information. How material is accessed and received should come into play when journalists and news organizations—measuring against ethical standards—decide how to treat certain information. The race to publish emails stolen from an individual's account and laundered through WikiLeaks creates a dangerous precedent. The press needs to treat stolen and laundered information with a high degree of caution and skepticism, similar to how it has treated the publication of the Christopher Steele dossier on Trump's Russia ties—refusing to report on some elements and prefacing any mention of the dossier as being "unverified."[127] For instance, ahead of its recent presidential elections and following the leaking of documents allegedly stolen from the Macron campaign, France's electoral commission called on the media not to cover the content of the leaked materials, warning that "the dissemination of such data, which has been fraudulently obtained and in all likelihood may have been mingled with false information, is liable to be classified as a criminal offense." As a result, the French media largely complied with the commission's request, including such major outlets as *Le Monde*.[128]

In a climate of fake news, there is a great need to cultivate news media that is independent of outside funding sources abroad. The same is true within the United States. The United States should increase investments into PBS and NPR.

The United States must stand up for democracy and human rights

Combating disinformation is also about standing up in support of freedom and democracy around the world at the highest levels of the U.S. government. Unfortunately, the Trump administration has not only failed to speak up for democracy and human rights, but it has also actively sought to undermine these values and what America stands for by, for instance, hosting Russian Foreign Minister Sergey Lavrov at the White House days after Russian interference in the French election—as well as ignoring human rights abuses and inviting President of the Philippines Rodrigo Duterte to the White House.[129] The Trump administration has bent over backward to accommodate and offer support to authoritarian governments and strongman rulers. Moreover, Trump's attack on the press, Secretary of State Tillerson's unwillingness to allow the press to travel

with him, the abandonment of the State Department's daily press briefing, and rhetoric about locking up political opponents cause tremendous damage to the moral authority of the United States and serve to weaken America's ability to lead.[130] When the leader of the free world no longer values democracy, these principles are weakened worldwide.

Conclusion

The unprecedented Russian interference in the 2016 election requires a strong and robust American response. As then-FBI Director James Comey explained in testimony before the House Intelligence Committee about Russian intentions, "[T]hey'll be back. And they'll be in 2020, they may be back in 2018" because "they were successful … they introduced chaos and division and discord and sewed doubt about the nature of this amazing country of ours and our democratic process."[131] If the United States continues to do nothing, foreign interference in American democracy will become the new normal. How the United States responds in the coming days, months, and years to this challenge will determine the future course of American democracy. It is a challenge that the United States cannot fail to meet.

About the authors

Max Bergmann is a senior fellow on the National Security and International Policy team at the Center for American Progress.

Carolyn Kenney is a policy analyst with the National Security and International Policy team at the Center.

Endnotes

1 Stephen Kotkin, "Russia's Perpetual Geopolitics," *Foreign Affairs*, May/June 2016, available at https://www.foreignaffairs.com/articles/ukraine/2016-04-18/russias-perpetual-geopolitics.

2 Lukasz Kulesa, "Russia and the West: Russia's Recent Assertiveness, Western Response, and What the Future May Hold," *Harvard International Review* 37 (4) (2016), available at http://hir.harvard.edu/russia-and-west-assertiveness-response-what-the-future-may-hold/.

3 Eugene Rumer, "Russia and the Security of Europe" (Washington: Carnegie Endowment for International Peace, 2016), available at http://carnegieendowment.org/2016/06/30/russia-and-security-of-europe-pub-63990.

4 PressTV, "Putin Calls for End to Political Killings in Russia," March 4, 2015, available at http://www.presstv.ir/Detail/2015/03/04/400287/Putin-calls-for-end-to-political-killings.

5 Shaun Walker, "Ukraine Set to Sign EU Pact that Sparked Revolution," *The Guardian*, June 26, 2014, available at https://www.theguardian.com/world/2014/jun/26/ukraine-european-union-trade-pact.

6 BBC News, "Ukraine Crisis: Timeline," November 13, 2014, available at http://www.bbc.com/news/world-middle-east-26248275.

7 Steven Pifer, "Ukraine, Russia and the U.S. Policy Response," Testimony before the Senate Foreign Relations Committee, June 5, 2014, available at https://www.brookings.edu/testimonies/ukraine-russia-and-the-u-s-policy-response/.

8 Samuel Charap and Jeremy Shapiro, "Consequences of a new Cold War," *Survival*, April-May 2015, available at https://www.iiss.org/en/publications/survival/sections/2015-1e95/survival--global-politics-and-strategy-april-may-2015-96a3/57-2-04-charap-and-shapiro-cm-8ce2.

9 Reuters, "Obama says Russia sanctions must stay in place until Minsk implemented," April 25, 2016, available at http://www.reuters.com/article/us-usa-germany-obama-russia-idUSKCN0XM10K.

10 Paul Sonne, "With 'Novorossiya,' Putin Plays the Name Game with Ukraine," *The Wall Street Journal*, September 1, 2014, available at https://www.wsj.com/articles/with-novorossiya-putin-plays-the-name-game-with-ukraine-1409588947.

11 Ishaan Tharoor, "After Clinton, Trump's real enemy is globalism," *The Washington Post*, November 3, 2016, available at https://www.washingtonpost.com/news/worldviews/wp/2016/10/28/how-globalism-became-the-boogeyman-of-2016/?utm_term=.2fd81ecbed80.

12 Heather A. Conley and others, "The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe," Center for Strategic and International Studies, October 13, 2016, available at https://www.csis.org/analysis/kremlin-playbook.

13 Ken Gude, "Russia's 5th Column" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/.

14 In the early 19th century, following Napoleon's defeat, the United States was also subject to thinly veiled Russian threats over its democratic status. In November 1823, Russian Ambassador to Washington Baron Tuyll passed a note to Secretary of State John Quincy Adams warning that St. Petersburg rejoiced "over the fallen cause of revolution" in Portugal and Spain and maintained "sturdy promises of determination to keep it down." In an address to Congress weeks later, President James Monroe responded to Tuyll and other threats of European encroachment by laying out what would later be called the Monroe Doctrine. See Charles Edel, *Nation-Builder: John Quincy Adams and the Grand Strategy of the Republic* (Cambridge, MA: Harvard University Press, 2014), pp. 174–181.

15 David Ignatius, "Russia's radical new strategy for information warfare," *The Washington Post*, January 18, 2017, available at https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.9377364417da.

16 U.S. Information Agency, "Soviet Active Measures in the 'Post-Cold War' Era 1988-1991," June 1992, available at http://intellit.muskingum.edu/russia_folder/pcw_era/index.htm.

17 Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," Hearing before U.S. Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf. Rid is citing Ladislav Bittman, *The KGB and Soviet Disinformation. An Insider's View* (Washington: Pergamon-Brassey's, 1985).

18 Leon Aron, "Russian Subversion of Western democracies is old news," AEIdeas, January 6, 2017, available at http://www.aei.org/publication/russian-hacking-subversion-of-western-democracies-old-news/.

19 Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," Hearing before U.S. Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

20 Max Seddon, "Documents Show How Russia's Troll Army Hit America," BuzzFeed, June 2, 2014, available at https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.kuy8V4gQJd#.vqopXNJyAd.

21 Massimo Calabresi, "Inside Russia's Social Media War on America," *Time*, May 18, 2017, available at http://time.com/4783932/inside-russia-social-media-war-america/.

22 Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money" (New York: Institute of Modern Russia, 2014), available at https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

23 Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, August 28, 2016, available at https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0.

24 Kulesa, "Russia and the West."

25 Taylor Wofford, "Russian State Media Says CIA Shot Down Malaysia Airlines Flight MH17," *Newsweek*, July 22, 2014, available at http://www.newsweek.com/russian-state-media-says-cia-shot-down-malaysian-airlines-flight-mh-17-260381.

26 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Executive Office of the President, 2017), available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

27 Ed Adamczyk, "Russia has a cyber army, defense minister acknowledges," UPI, February 23, 2017, available at http://www.upi.com/Top_News/World-News/2017/02/23/Russia-has-a-cyber-army-defense-minister-acknowledges/2421487871815/. See also Emmanuel Grynszpan, "Russian official: Information war part of 'battle of consciousness of the masses'," EurActiv, February 28, 2017, available at http://www.euractiv.com/section/global-europe/news/russian-official-information-war-part-of-battle-for-the-consciousness-of-the-masses/.

28 Ibid.

29 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

30 See Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." In War on the Rocks, Andrew Weisburd, Clint Watts, and JM Berger similarly refer to this as White, Grey, and Black. See Andrew Weisburd, Clint Watts, and JM Berger, "Trolling for Trump: How Russia is Trying to Destroy Our Democracy," War on the Rocks, November 6, 2016, available at https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

31 Caitlin Patterson, "Russia's Surging Electronic Warfare Capabilities," *The Diplomat*, April 19, 2016, available at http://thediplomat.com/2016/04/russias-surging-electronic-warfare-capabilities/.

32 Doina Chiacu and Arshad Mohammed, "Leaked audio reveals embarrassing U.S. exchange on Ukraine, EU," Reuters, February 6, 2014, available at http://www.reuters.com/article/us-usa-ukraine-tape-idUSBREA1601G20140207.

33 Michael Fuchs and others, "Why Americans Should Care About Russian Hacking" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/security/reports/2017/02/14/415073/why-americans-should-care-about-russian-hacking/.

34 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

35 Andrea Shalal, "Germany challenges Russia over alleged cyberattacks," Reuters, May 4, 2017, available at http://www.reuters.com/article/us-germany-security-cyber-russia-idUSKBN1801CA.

36 Christopher Dickey, "Fighting Back Against Putin's Hackers," *The Daily Beast*, April 25, 2017, available at http://www.thedailybeast.com/articles/2017/04/25/fighting-back-against-putin-s-hackers.

37 Sam Jones and Max Seddon, "Licensed to Hack: The Rise of the Cyber Privateer," *Financial Times*, March 16, 2017, available at https://www.ft.com/content/21be48ec-0a48-11e7-97d1-5e720a26771b.

38 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

39 Both Cozy Bear and Fancy Bear hacked the DNC, and Fancy Bear was found to be behind the Podesta email hack. For more information, see Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, available at https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

40 Rebecca Shabad, "Russian 'fingerprints' left behind on DNC hack," CBS News, July 26, 2016, available at http://www.cbsnews.com/news/russian-fingerprints-left-behind-on-dnc-hack/; CBS News, "AP: Hacked emails show Democratic Party hostility to Bernie Sanders," July 23, 2016, available at http://www.cbsnews.com/news/ap-hacked-emails-show-democratic-party-hostility-to-bernie-sanders/.

41 Rick Noack, "Cyberattack on French presidential front-runner bears Russian 'fingerprints,' research group says," *The Washington Post*, April 25, 2017, available at https://www.washingtonpost.com/news/worldviews/wp/2017/04/25/cyberattack-on-french-presidential-front-runner-bears-russian-fingerprints-research-group-says/?utm_term=.c47da147720b.

42 Sheera Frenkel, "It Looks Like Someone Curated the Wikileaks Emails Before They Were Published," BuzzFeed, February 3, 2017, available at https://www.buzzfeed.com/sheerafrenkel/it-looks-like-someone-curated-the-wikileaks-emails-before-th?utm_term=.otQb0M9dgr#.okrNR3B9Mo.

43 Aaron Sharockman, "It's True: WikiLeaks Dumped Podesta Emails Hour after Trump Video Surfaced," PolitiFact, December 18, 2016, available at http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta/its-true-wikileaks-dumped-podesta-emails-hour-afte/. For the exact timing of the releases, see the Center for American Progress Action Fund's Moscow Project at www.themoscowproject.org.

44 Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns."

45 David Leionhardt, "A French Lesson for the American Media," *The New York Times*, May 9, 2017, available at https://www.nytimes.com/2017/05/09/opinion/a-french-lesson-for-the-american-media.html?ref=opinion&_r=0.

46 Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns."

47 Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015, available at https://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

48 Seddon, "Documents Show How Russia's Troll Army Hit America."

49 Scott Gelbach and Konstantin Sonin, "Trump helps Putin – and all dictators – when he calls U.S. elections 'rigged'," *The Washington Post*, October 26, 2016, available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/26/putin-wins-when-trump-says-u-s-elections-are-rigged-so-do-all-dictators/?utm_term=.96f1cfa7859a.

50 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

51 Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation," *The New York Times*, May 30, 2016, available at https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html.

52 Ibid.

53 Ben Nimmo, "Anatomy of Info-War: How Russia's Propaganda Machine Works, and How to Counter It," StopFake.Org, May 19, 2015, available at http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

54 Weisburd, Watts, and Berger, "Trolling for Trump."

55 Jonathon Morgan and Kris Shaffer, "Sockpuppets, Secessionists, and Breitbart," Medium, March 31, 2017, available at https://medium.com/data-for-democracy/sockpuppets-secessionists-and-breitbart-7171b1134cd5.

56 Craig Timberg, "As a conservative Twitter user sleeps, his account is hard at work," *The Washington Post*, February 5, 2017, available at https://www.washingtonpost.com/business/economy/as-a-conservative-twitter-user-sleeps-his-account-is-hard-at-work/2017/02/05/18d5a532-df31-11e6-918c-99ede3c8cafa_story.html?utm_term=.d82e02d57e4d.

57 MacFarquhar, "A Powerful Russian Weapon."

58 Samantha Subramanian, "Inside the Macedonian Fake-News Complex," *Wired*, February 15, 2017, available at https://www.wired.com/2017/02/veles-macedonia-fake-news/.

59 See Secured Borders Facebook page, available at https://www.facebook.com/Secured.Borders/ (last accessed May 2017).

60 Alexey Kovalev, "Russia's Infamous 'Troll Factory' Is Now Posing as a Media Empire," *The Moscow Times*, March 24, 2017, available at https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534.

61 Gideon Resnick, "How Pro-Trump Twitter Bots Spread Fake News," *The Daily Beast*, November 17, 2016, available at http://www.thedailybeast.com/articles/2016/11/17/how-pro-trump-twitter-bots-spread-fake-news.html.

62 Bench Kollanyi, Philip N. Howard, and Samuel C. Woolley, "Bots and Automation Over Twitter During the U.S. Election" (Oxford, United Kingdom: Oxford University, 2016), available at http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf.

63 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

64 Marcus Gilmer, "Army of Russian trolls reportedly targeted swing states with anti-clinton fake news," Mashable, March 30, 2017, available at http://mashable.com/2017/03/30/russian-trolls-fake-news/#6fMj0yS_fPq3.

65 Calabresi, "Inside Russia's Social Media War on America."

66 For instance, see Political Bots, an Oxford University project that has been investigating political bots and other forms of online propaganda since 2012, available at http://comprop.oii.ox.ac.uk/ (last accessed April 2017).

67 Nimmo, "Anatomy of an Info-War."

68 Zack Beauchamp, "The Russian government just tweeted an image of a white supremacist frog," Vox, January 9, 2017, available at http://www.vox.com/world/2017/1/9/14212496/russia-embassy-pepe.

69 Kate Starbird, "Information Wars: A Window into the Alternative Media Ecosystem," Medium, March 14, 2017, available at https://medium.com/hci-design-at-uw/information-wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f.

70 Gude, "Russia's 5th Column."

71 Peter Stone and Greg Gordon, "FBI's Russian-influence probe includes a look at Breitbart, InfoWars news sites," McClatchy, March 20, 2017, available at http://www.mcclatchydc.com/news/politics-government/white-house/article139695453.html.

72 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections"*; Simon Shuster, "Inside Putin's On-Air Machine," *Time*, March 5, 2015, available at http://time.com/rt-putin/.

73 Dana Priest and Greg Miller, "He was one of the most respected intel officers of his generation. Now he's leading 'lock her up' chants," *The Washington Post*, August 15, 2016, available at https://www.washingtonpost.com/world/national-security/nearly-the-entire-national-security-establishment-has-rejected-trumpexcept-for-this-man/2016/08/15/d5072d96-5e4b-11e6-8e45-477372e89d78_story.html?utm_term=.90d1d8cd7d42.

74 Catherine Taibi, "Russia Today Anchor Resigns, Admits To Spreading 'Lies' For Putin," The Huffington Post, July 18, 2014, available at http://www.huffingtonpost.com/2014/07/18/sara-firth-resigns-russia-today-lies-anchor_n_5598815.html.

75 Paul Farhi, "How Ed Schultz transformed from MSNBC lefty to the American face of Moscow media," *The Washington Post*, December 20, 2016, available at https://www.washingtonpost.com/lifestyle/style/how-ed-schultz-transformed-from-msnbc-lefty-to-the-american-face-of-moscow-media/2016/12/20/320713f4-c322-11e6-8422-eac61c0ef74d_story.html?utm_term=.9e375a48dab2.

76 Pomerantsev and Weiss, "The Menace of Unreality."

77 Clint Watts and Andrew Weisburd, "How Russia Dominates Your Twitter Feed to Promote Lies (And, Trump, Too)," *The Daily Beast*, August 6, 2016, available at http://www.thedailybeast.com/articles/2016/08/06/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.

78 Linda Qiu, "Trump campaign chair misquotes Russian media in bogus claim about NATO base terrorist attack," PolitiFact, August 16, 2016, available at http://www.politifact.com/truth-o-meter/statements/2016/aug/16/paul-manafort/trump-campaign-chair-misquotes-russian-media-makes/.

79 Matthew Nussbaum, "How the U.K. spying claim traveled from an ex-CIA blogger to Trump's White House," *Politico*, March 18, 2017, available at http://www.politico.com/story/2017/03/trump-gchq-spying-larry-johnson-intelligence-community-236220.

80 Chen, "The Agency."

81 David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *The New York Times*, December 29, 2016, available at https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=0.

82 Nicole Gaudiano, "GOP blocks House vote on independent Russia-Trump investigation," *USA Today*, May 17, 2017, available at https://www.usatoday.com/story/news/politics/2017/05/17/gop-blocks-house-vote-independent-russia-trump-probe/101796632/.

83 Tom LoBianco, "Senate Russia hearing: Rubio divulges hack attempts," CNN, March 31, 2017, available at http://www.cnn.com/2017/03/30/politics/senate-intelligence-committee-hearing-russia/.

84 Mary Papenfuss, "Here We Go Again: Russia Accused Of Cyberattacks In Another Election," The Huffington Post, February 20, 2017, available at http://www.huffingtonpost.com/entry/russia-election-hack_us_58aa6654e4b07602ad55f562; Cecile Vaissie, "Can the Kremlin Influence the French Election?", *The New York Times*, April 14, 2017, available at https://www.nytimes.com/2017/04/14/opinion/can-the-kremlin-influence-the-french-election.html?_r=0.

85 Theresa Lageman, "Russian Hackers Use Dutch Polls as Practice," DW, March 10, 2017, available at http://www.dw.com/en/russian-hackers-use-dutch-polls-as-practice/a-37850898.

86 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *The New York Times*, February 16, 2017, available at https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html?_r=0.

87 Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption," *The New York Times*, December 8, 2016, available at https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html.

88 Arthur Beesley, "EU Suffers Jump in Aggressive Cyber Attacks," *Financial Times*, January 8, 2017, available at https://www.ft.com/content/3a0f0640-d585-11e6-944b-e7eb37a6aa8e.

89 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections."*

90 Jose Pagliery, "Russian money-laundering details remain in the dark as US settles fraud case," CNN, May 13, 2017, available at http://www.cnn.com/2017/05/13/world/prevezon-settlement/.

91 Austin Wright, "Corker: We're not going to do a Russia sanctions bill," *Politico*, May 1, 2017, available at http://www.politico.com/story/2017/05/01/corker-russia-sanctions-senate-237855.

92 C-SPAN, "Clinton Watts. Senate Intelligence Committee Hearing," March 30, 2017, available at https://www.c-span.org/video/?c4664379/clinton-watts-senate-intelligence-committee-hearing.

93 Department of Homeland Security Press Office, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," Press release, October 7, 2016, available at https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

94 John P. Carlin, "The Russians Are Coming. Again.", *Politico Magazine*, April 6, 2017, available at http://www.politico.com/magazine/story/2017/04/russia-foreign-meddling-american-democracy-214994.

95 Christopher Dickey, "Did Macron Outsmart Campaign Hackers?", *The Daily Beast*, May 6, 2017, available at http://www.thedailybeast.com/articles/2017/05/06/did-macron-outsmart-campaign-hackers.

96 James Savridis, "How to Win the Cyberwar Against Russia," *Foreign Policy*, October 12, 2016, available at http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

97 Shalal, "Germany challenges Russia over alleged cyber-attacks."

98 Katie Bo Williams, "Dems: New Geneva Conventions needed for cyber war," The Hill, September 10, 2015, available at http://thehill.com/policy/cybersecurity/253231-dems-new-geneva-conventions-needed-for-cyber-war.

99 Obama White House Office of the Press Secretary, "FACT SHEET: The 2016 G-20 Summit in Hangzhou, China," Press release, September 5, 2016, available at https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/fact-sheet-2016-g-20-summit-hangzhou-china.

100 Mary Beth Sheridan, "Obama secures 47-nation pact at nuclear summit," *The Washington Post*, April 14, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/04/13/AR2010041300427.html.

101 Jon Sharman, "Vladimir Putin was 'really clear' with Obama when confronted over US election hack," *The Independent*, December 17, 2016, available at http://www.independent.co.uk/news/world/americas/vladimir-putin-really-clear-barack-obama-us-election-hack-g20-cut-it-out-a7481686.html.

102 C-SPAN, "Clinton Watts. Senate Intelligence Committee Hearing."

103 European External Action Service, "Questions and Answers about the East StratCom Task Force," January 14, 2017, available at https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/%20Questions%20and%20Answers%20about%20the%20East%20StratCom%20Task%20Force.

104 Disinformation Review, "How Pro-Kremlin Outlets Abuse the Tragedy of Terror," April 16, 2017, available at https://euvsdisinfo.eu/how-pro-kremlin-outlets-abuse-the-tragedy-of-terror/.

105 Kavitha Surana, "The EU Moves to Counter Russian Disinformation Campaign," *Foreign Policy*, November 23, 2016, available at http://foreignpolicy.com/2016/11/23/the-eu-moves-to-counter-russian-disinformation-campaign-populism/.

106 Agamoni Ghosh, "Google sends state-sponsored hack warnings to numerous journalists and professors," *International Business Times*, November 24, 2016, available at http://www.ibtimes.co.uk/google-sends-state-sponsored-hack-warnings-numerous-journalists-professors-1593172.

107 Elias Groll, "DOJ Charges Russian Intelligence in Huge Yahoo Hack," *Foreign Policy*, March 15, 2017, available at http://foreignpolicy.com/2017/03/15/doj-charges-russian-intelligence-in-huge-yahoo-hack/?utm_content=buffer36bab&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

108 U.S. Senate Committee on Armed Services, "Hearing to Receive Testimony on Foreign Cyber Threats to the United States," January 5, 2017, available at https://www.armed-services.senate.gov/imo/media/doc/17-01_01-05-17.pdf.

109 Ingrid d'Hooghe, "The Expansion of China's Public Diplomacy System." In J. Wang, ed., *Soft Power in China: Public Diplomacy through Communication* (Basingstoke, United Kingdom: Palgrave Macmillan, 2011).

110 Center for Euro-Atlantic Studies, "Eyes Wide Shut – Russian Soft Power Gaining Strength in Serbia: Goals, Instruments, and Effects" (2016), available at https://www.ceas-serbia.org/images/2016/04/EYES_WIDE_SHUT_-_EXECUTIVE_SUMMARY.pdf.

111 U.S. Global Leadership Coalition, "Deep and Dangerous Cuts to International Affairs Budget Would Make America Less Safe" (2017), available at http://www.usglc.org/downloads/2017/03/USGLC-FY18-Budget-Analysis.pdf. For the Trump administration's budget submission, see The White House, "President Trump's Taxpayer First Budget," available at https://www.whitehouse.gov/taxpayers-first (last accessed May 2017).

112 CBS News, "U.S. launches TV network as alternative to Russian propaganda," February 9, 2017, available at http://www.cbsnews.com/news/us-current-time-tv-network-rfe-russia-russian-propaganda-misinformation-rt/.

113 Tim Mak, "U.S. Preps for Infowar on Russia," *The Daily Beast*, February 6, 2017, available at http://www.thedailybeast.com/articles/2017/02/06/u-s-preps-for-infowar-on-russia.html.

114 U.S. Department of State, "Global Engagement Center," available at https://www.state.gov/r/gec/ (last accessed April 2017).

115 Josh Rogin, "Inside the Public Relations Disaster at the Cairo Embassy," *Foreign Policy*, September 12, 2012, available at http://foreignpolicy.com/2012/09/12/inside-the-public-relations-disaster-at-the-cairo-embassy/.

116 Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook" (Menlo Park, CA: Facebook, 2017), available at https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

117 Elle Hunt, "'Disputed by multiple fact-checkers': Facebook rolls out new alert to combat fake news," *The Guardian*, March 21, 2017, available at https://www.theguardian.com/technology/2017/mar/22/facebook-fact-checking-tool-fake-news?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+USA+-+Collections+2017&utm_term=218505&subid=18917142&CMP=GT_US_collection.

118 Craig Silverman, "Facebook Changed Its Trending Product to Make It Show the Same Stuff to Everyone," BuzzFeed, January 25, 2017, available at https://www.buzzfeed.com/craigsilverman/facebook-is-tweaking-its-trending-product?utm_term=.odOJQ15Mk#.rePxw6Zqe.

119 Anick Jesdanun, "Google expands fact checking in news searches," Associated Press, April 7, 2017, available at https://apnews.com/8af39d8b7c404e1bbeb9cdcc3e4475d4.

120 Nick Wingfield, Mike Isaac, and Katie Benner, "Google and Facebook Take Aim at Fake News Sites," *The New York Times*, November 14, 2016, available at https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html.

121 Scott Spencer, "How we fought bad ads, sites and scammers in 2016," Google Ads blog, January 25, 2017, available at https://blog.google/topics/ads/how-we-fought-bad-ads-sites-and-scammers-2016/.

122 Clint Watts and Andrew Weisburd, "Can the Michelin Model Fix Fake News?", *The Daily Beast*, January 22, 2017, available at http://www.thedailybeast.com/articles/2017/01/22/can-the-michelin-model-fix-fake-news.html.

123 Michael Newberg, "As many as 48 million Twitter accounts aren't people, says study," CNBC, March 10, 2017, available at http://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html.

124 Dave Gershgorn, "There's a new tool to visualize how fake news is spread on Twitter," Quartz, December 21, 2016, available at https://qz.com/869344/theres-a-new-tool-to-visualize-how-fake-news-is-spread-on-twitter/.

125 Indiana University, "IU Computer Scientists Develop Tool for Uncovering Bot-Controlled Twitter Accounts," Press release, May 6, 2014, available at http://archive.news.indiana.edu/releases/iu/2014/05/twitter-botornot.shtml.

126 Joseph Lu, "Twitter Bot Scandal Puts Further Pressure on CEO Jack Dorsey," Zacks, March 20, 2017, available at https://www.zacks.com/stock/news/253426/twitter-bot-scandal-puts-further-pressure-on-ceo-jack-dorsey.

127 See, for instance, Scott Shane, Nicholas Confessore, and Matthew Rosenberg, "How a Sensational, Unverified Dossier Became a Crisis for Donald Trump," *The New York Times*, January 11, 2017, available at https://www.nytimes.com/2017/01/11/us/politics/donald-trump-russia-intelligence.html.

128 Amanda Erickson, "Macron's emails got hacked. Here's why French voters won't hear much about them before Sunday's election.", *The Washington Post*, May 6, 2017, available at https://www.washingtonpost.com/news/worldviews/wp/2017/05/06/macrons-emails-got-hacked-heres-why-french-voters-wont-hear-much-about-them-before-sundays-election/?utm_term=.c7673ce62f7a.

129 The LA Times Editorial Board, "Philippine President Duterte is a self-professed killer. Why did Trump invite him to a cozy White House schmooze?", *Los Angeles Times*, May 2, 2017, available at http://www.latimes.com/opinion/editorials/la-ed-trump-duterte-white-house-20170502-story.html.

130 Julie Hirschfeld Davis and Michael M. Grynbaum, "Trump Intensifies His Attacks on Journalists and Condemns F.B.I. 'Leakers'," *The New York Times*, February 24, 2017, available at https://www.nytimes.com/2017/02/24/us/politics/white-house-sean-spicer-briefing.html; Mark Hensch, "Tapper: Tillerson traveling without press 'insulting'," The Hill, March 9, 2017, available at http://thehill.com/policy/international/asia-pacific/323205-tapper-tillerson-traveling-without-press-insulting; Anne Gearan, "State Department press briefing canceled because of travel order," *The Washington Post*, March 6, 2017, available at https://www.washingtonpost.com/news/post-politics/wp/2017/03/06/state-department-press-briefing-canceled-because-of-travel-order/?utm_term=.42a714e0c8f8.

131 The Washington Post Staff, "Full transcript: FBI Director James Comey testifies on Russian interference in 2016 election," *The Washington Post*, March 20, 2017, available at https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.a268f7d57c64.

Our Mission

The Center for American Progress is an independent, nonpartisan policy institute that is dedicated to improving the lives of all Americans, through bold, progressive ideas, as well as strong leadership and concerted action. Our aim is not just to change the conversation, but to change the country.

Our Values

As progressives, we believe America should be a land of boundless opportunity, where people can climb the ladder of economic mobility. We believe we owe it to future generations to protect the planet and promote peace and shared global prosperity.

And we believe an effective government can earn the trust of the American people, champion the common good over narrow self-interest, and harness the strength of our diversity.

Our Approach

We develop new policy ideas, challenge the media to cover the issues that truly matter, and shape the national debate. With policy teams in major issue areas, American Progress can think creatively at the cross-section of traditional boundaries to develop ideas for policymakers that lead to real change. By employing an extensive communications and outreach effort that we adapt to a rapidly changing media landscape, we move our ideas aggressively in the national policy debate.

Center for American Progress

1333 H STREET, NW, 10TH FLOOR, WASHINGTON, DC 20005 • TEL: 202-682-1611 • FAX: 202-682-1867 • WWW.AMERICANPROGRESS.ORG