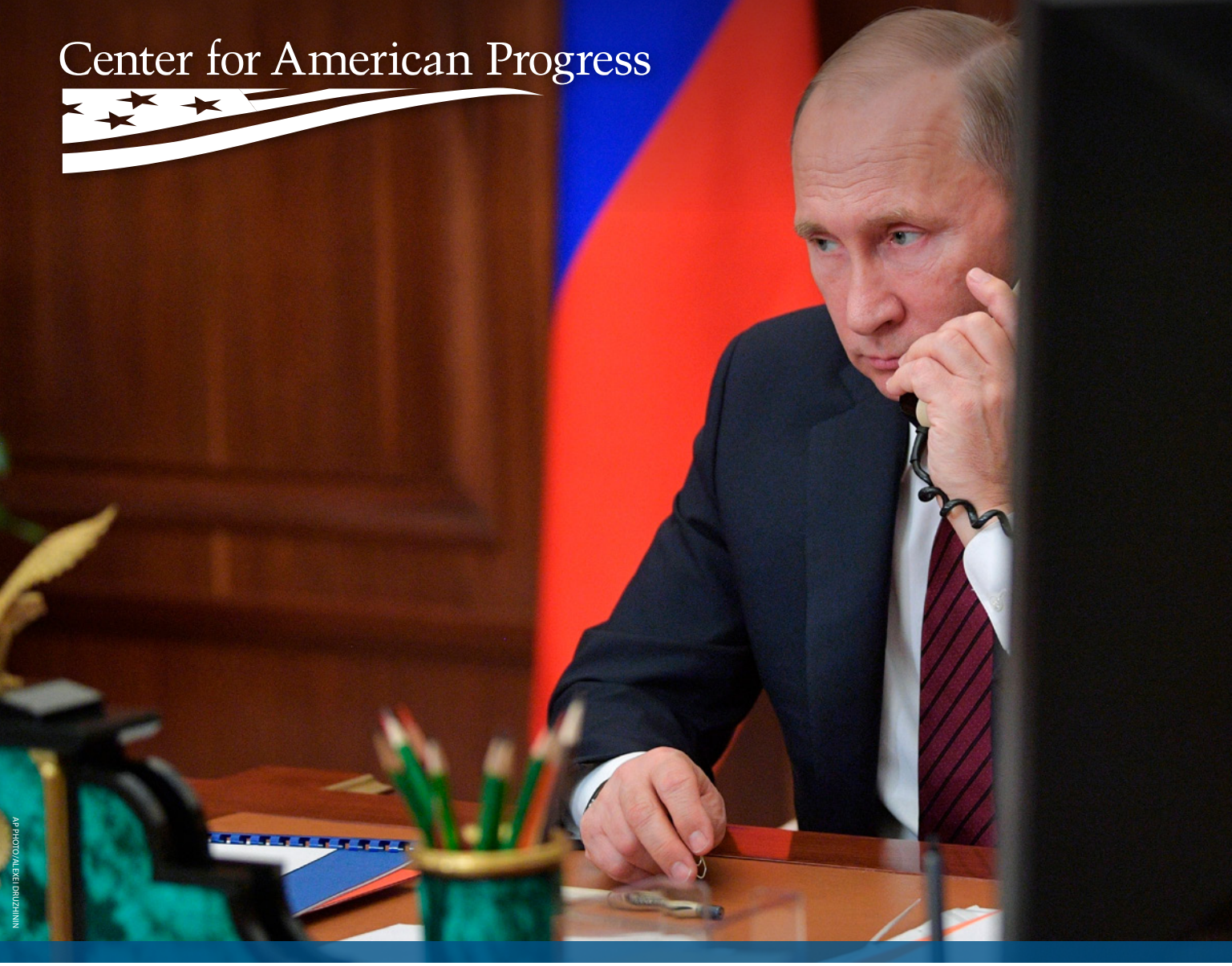
Center for American Progress



AP PHOTO/ALEXEI DRUZHININ

Acts of an Adversary

Russia's Ongoing Hostilities Toward the United States and Its Allies

By Max Bergmann and Carolyn Kenney December 2017

Center for American Progress

Acts of an Adversary

Russia's Ongoing Hostilities Toward the United States and Its Allies

By Max Bergmann and Carolyn Kenney December 2017

Contents

1 Introduction and summary

6 Russia is aggressively attacking and spying on the United States in cyberspace

12 Russia's continuing espionage efforts against the United States

18 Russia is probing ways to attack America

21 Russian continues to intervene in American politics

25 Russia undermining international law and treaties

28 Russian military operating dangerously and provocatively

30 Russia acting against U.S. interests and international stability worldwide

32 Recommendations

38 Conclusion

40 Endnotes

Introduction and summary

Russia's efforts to attack and undermine American democracy did not begin or end with the 2016 election. Russia's vast espionage and cybercapabilities continue to target the United States government, its citizens, as well as America's democratic allies around the world.

This report outlines Russia's continuing hostile actions toward the United States and its allies. It finds that the election of Donald Trump has not resulted in the Kremlin changing course or reducing its hostile actions toward the United States. Russia continues to:

- Aggressively target the United States in cyberspace, including its government, businesses, citizens, and interests
- Provide cybercriminals with a safe haven from which they can prey on Americans
- Conduct aggressive espionage campaigns against the United States and its allies, including harassing U.S. diplomats and assassinating the Kremlin's adversaries abroad
- Probe ways to attack American infrastructure, especially in the energy, communications, and financial sectors
- Intervene in American elections, politics, and political discourse, often by utilizing social media platforms
- Operate dangerously and provocatively against U.S. and NATO forces
- Occupy territory of a sovereign foreign country in violation of fundamental principles of international law
- Act against U.S. interests worldwide

These are not the actions of an ally; they are the actions of an adversary. The Kremlin has made a strategic determination that the United States is an adversary—not an ally or partner—of Russia. This is a determination based not on who holds the White House but rather on what America stands for and represents. The Kremlin has shifted back to a Cold War-footing; has brushed off and updated much of the playbook of the Soviet Union; and is seeking to undermine democratic states from within.[1] Yet the Russian Federation is not the Soviet Union.

Modern Russia is, in fact, comparatively weak economically and has nowhere near the diplomatic and military clout of the Soviet Union during the Cold War. As a result, Russia operates in a more insurgent manner, using asymmetric means to undermine the United States, NATO, and the European Union.

Despite Russia's blatant attack on American democracy during the 2016 election, President Trump and Secretary of State Rex Tillerson have pursued a policy of appeasement. Throughout his political campaign and first year in office, Trump has never wavered from bestowing praise on Russian President Vladimir Putin. Trump has repeatedly cast doubt on the intelligence community's assessment that the Russian government intervened in the U.S. election. During his recent trip to Asia, Trump told reporters, "Every time he [Putin] sees me, he says, 'I didn't do that,' and I really believe that when he tells me that."[2] This statement, even though the White House tried to walk it back, is incredibly dangerous for the United States.[3] It provides a significant opening for Russia, as it indicates that the United States now has a president who is inclined to believe Putin, a former KGB agent, over members of the U.S. intelligence community, who have taken an oath to defend and protect the United States.

Instead of taking steps to protect America and respond to Russian efforts, President Trump and Secretary of State Tillerson have sought to establish a strategic alliance with Russia. Trump has suggested the creation of a "cyber security unit" with Russia, despite Russia serving as a safe haven for cybercriminals.[4] He has also sought to cooperate with Russia on counterterrorism in Syria, despite Russia's focus on propping up the regime.[5] What seems lost on the White House is that a "grand bargain" is in Russia's interests, not the United States', as Russia simply has little to offer the United States short of a dramatically changing its behavior. Russia's economy is relatively small and sputtering, and its major economic asset, its vast fossil fuel energy resources, have little strategic interest to the United States, which is now awash in natural gas, transitioning to more renewable sources of energy, and is benefitting from low global energy prices. While there are some areas of mutual interest where it is prudent to cooperate with Russia, such as nuclear arms control and nonproliferation, any broader rapprochement between the United States and Russia should require a dramatic change in the Kremlin's behavior, something Russia has not signaled any interest in pursuing and the Trump administration has not even sought.

The White House and secretary of state are also effectively weakening America's defenses by taking steps that undermine efforts to oppose Russian aggression, both domestically and abroad. Such steps include the following:

- The Trump administration has sought to remove sanctions related to Russia's actions in Ukraine
- The president and the secretary of state sought to block and then water down sanctions on Russia
- The secretary of state is deconstructing and downsizing the U.S. Department of State, gutting the ability of U.S. diplomacy to counter Russian influence
- The president and the secretary of state hosted the Russian Foreign Minister Sergey Lavrov at the White House and State Department just days after Russian interference in the French election[6]
- The secretary of state recently closed the State Department's office responsible for overseeing and coordinating U.S. sanctions across various government agencies, even though the administration now has to implement a massive Russian sanctions bill[7]
- The secretary of state has slowed and constrained the ability of the Global Engagement Center to counter Russian influence operations around the world
- The president and secretary of state, by downplaying support for democracy and human rights, have hobbled efforts to counter Russian propaganda, especially in Eastern Europe

This weakness in the face of Russian aggression only invites future attacks on America. Former FBI Director James Comey testified in March 2017 that Russia is not done: "They'll be back. And they'll be in 2020, they may be back in 2018 … [T]hey were successful."[8] The United States must face the reality that as long as Vladimir Putin is leading Russia, the United States and Russia will be strategic adversaries.

This summer, with near unanimity, the U.S. congress passed bipartisan Russia sanctions legislation that could impose real costs on Russia for its interference in the 2016 election. Congress must now make sure that the administration is actually implementing the sanctions legislation. However, while imposing costs on Russia is essential, Congress also needs to take action now to protect our democracy from future attacks. Currently, the Republican-controlled Congress has also done little to protect America from the ongoing threat posed by Russia. Despite Russia's attack on American democracy, the Republican-controlled Congress

has not called out the White House for its inaction and its efforts to appease the Kremlin. Congress has passed no legislation to defend the country from future attack. America remains badly exposed, as important legislation to shore up the security of the election system remains blocked by Senate Majority Leader Mitch McConnell (R-KY) and House Speaker Paul Ryan (R-WI). The near unanimous support for Russia sanctions legislation shows there is bipartisan support for action should Congressional leadership allow legislation to come to a vote.

Despite the lack of concern from Congress and the White House, the U.S. military, U.S. diplomats, the intelligence community, the Department of Justice, the FBI, and many hardworking Americans within U.S. government agencies are taking steps to address the challenge. It is important to note that the United States therefore also conducts some of the same espionage practices that Russia is employing and that the United States spies on Russia, just as Russia spies on the United States. Similar to how the United States sees certain Russian actions as provocative, the Russians also see certain actions by the United States and its NATO allies as being just as provocative. This is not unusual, especially among countries that approach each other as adversaries. However, while Russia approaches the United States as an adversary, the inclination from the White House to appease the Kremlin has meant that there is no coherent policy from the Trump administration toward Russia. The absence of any U.S. diplomatic energy or direction from the secretary of state means that these agencies are trying to respond to Russia with one hand tied behind their back, as there is no leadership, no strategy, few resources, and no priority given to this challenge.

Furthermore, the Trump administration's incoherence creates a dangerous dynamic. The lack of clarity means the Kremlin does not know when it has gone too far or crossed the line because no line is drawn and no potential consequences were articulated. Russian efforts, therefore, have pushed further and further and frequently pushed the boundaries into areas that could be seen as hostile. Avoiding an escalatory cycle requires drawing clear lines. And while the United States and Russia need to be ever mindful of falling into an escalatory spiral, that does not mean the United States should seek to appease the Kremlin and cater to its grudges. The United States must stand up for itself and its allies and re-establish a level of deterrence with Russia so that Russia knows hostile acts against the United States and allies have consequences.

Reverting to an adversarial relationship with Russia is not an outcome the United States sought. Following the Cold War, U.S. strategy toward Russia was designed to integrate Russia into Europe and the West; not to recreate a new Cold War dynamic. While certain U.S. actions after the Cold War may have stoked grievances and fostered a belief in Moscow that the United States remained an adversary, again and again, through the presidencies of Clinton, Bush, and Obama, the United States sought to build positive relations with Russia and incorporate it into the international community. But while the U.S. sought to turn the page on the Cold War, Russia, under Putin, did not. Under Putin, Russia has more than just rejected these overtures—it has actively sought to undermine the United States, liberal democracy, and European unity.

This report seeks to outline the breadth of Russian efforts to undermine and compromise the United States. This documentation is not intended to be comprehensive. Instead, it is meant to be illustrative of the ways in which Russia is continuing to meddle, undermine, and attack the United States and its allies. While Russian efforts never shifted their focus from the United States after the Cold War, there was a clear shift in focus in the United States away from Russia and toward counterterrorism, the Middle East, and, now, China and Asia.[9] As this report will demonstrate, Russia's efforts to undermine the United States its allies are extensive, and to respond, the United States must shift its focus back toward countering the threat that Russia poses.

Russia is aggressively attacking and spying on the United States in cyberspace

A key theater for Russia's efforts against the United States is in cyberspace. Russia's attack on the election in the 2016 was, according to a U.S. Department of Homeland Security (DHS) and the FBI's joint assessment in December:

> *… part of an ongoing [Russian Intelligence Services] campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spear-phishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information.*[10]

Russia attacked U.S. election infrastructure in 2016

Russian efforts to interfere in the U.S. election system were much more extensive than previously believed. As Sen. Richard Burr (R-NC), the chair of the Senate intelligence committee, said on June 21, 2017, "There's no question that Russia carried out attacks on state election systems."[11] Bloomberg reported on June 13, 2017, that "Russia's cyberattack on the U.S. electoral system before Donald Trump's election was far more widespread than has been publicly revealed, including incursions into voter databases and software systems in almost twice as many states as previously reported."[12] In all, according to Bloomberg's sources, "Russian hackers hit systems in 39 states," while the DHS disclosed that at least 21 states were targeted.

At the time, these attacks were so concerning that the Obama administration used a modern-day "red phone" to confront Moscow about its attacks in October.[13] Nevertheless, after the election, President Barack Obama assured the nation in a press conference in December that, "[W]e did not see further tampering of the election process."[14] It is now apparent that that this was not correct; Russian efforts continued to Election Day.

Indeed, much of what the intelligence community is learning about the Russian attacks on our election system was not caught at the time but, instead, is being learned well-after. At a Senate intelligence committee hearing in June, it was revealed by Bill Priestap, the assistant director of the Counterintelligence Division of the FBI, that the FBI now has "a number of investigations open" and are "all still pending … [W]e continue to learn things" about what happened. On June 5, 2017, The Intercept published a top-secret report from the National Security Agency (NSA) that provided a window into Russia's efforts.[15] The report was based on intelligence learned in April 2017, well-after the election and Obama's statement. The intelligence revealed that:

> *Russian General Staff Main Intelligence Directorate actors … executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solution … The actors likely used data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations … In October 2016, the actors also created a new email address that was potentially used to offer election-related products and services, presumably to U.S.-based targets.*

The Intercept summarized that, "As described by the classified NSA report, the Russian plan was simple: pose as an e-voting vendor and trick local government employees into opening Microsoft Word documents invisibly tainted with potent malware that could give hackers full control over the infected computers."[16] The Russians therefore did not stop their efforts to interfere in the election system as President Obama believed they would. The attack effort outlined by the NSA document is just one incident that we have learned about. As Joe Hall, chief technologist at the Center for Democracy and Technology, explained, "If it was a dedicated campaign by the GRU, they're not going to settle for attacking one podunk vendor, they'll try many different things."[17]

Bloomberg further revealed, "In Illinois, investigators found evidence that cyber-intruders tried to delete or alter voter data."[18] Mark Graff, former chief cybersecurity officer at Lawrence Livermore National Lab, told The Intercept that this could be "effectively a denial of service attack" against potential voters.[19] Furthermore, as Vox's Timothy Lee concluded, "[G]aining access to voter registration systems could be a first step to hacking voting machines themselves."[20] Experts have also long warned that our election system is extremely vulnerable to cyberattack. As J. Alex Halderman, a professor of computer science and an election security expert

at the University of Michigan, noted in his prepared testimony before the Senate intelligence committee in June, "Cybersecurity experts have … found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk."[21]

Russia provides a haven for cybercriminals to prey on Americans

Russia serves as a haven for cybercrime against the West. According to a senior British intelligence official in an interview with the *Financial Times*, Moscow has "fostered a network of 'modern privateers,'" effectively emulating state-sanctioned piracy of centuries ago, where monarchs greenlit 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."[22] These criminal cyberactors are essentially allowed to operate unimpeded if they confine their criminal efforts outside Russia and serve the needs of the Kremlin when called upon. Moreover, these private hackers also give the Kremlin additional cyberfirepower and the ability to surge its efforts when needed. According to Brandon Valeriano, a researcher at the Marine Corps University, "Russia has complete control over their cyberspace … and they're perfectly happy to let [hackers] continue their criminal exercises as long as they're able to work for the state even part time."[23]

The FBI's Most Wanted cybercriminal lives with impunity in Russia

The FBI has a $3 million bounty for the capture of Evgeniy Bogachev, but he lives openly in the Russian Black Sea resort town of Anapa. He is alleged to have created, according to *The New York Times*, "a sprawling network of virus-infected computers to siphon hundreds of millions of dollars from bank accounts around the world, targeting anyone with enough money worth stealing — from a pest control company in North Carolina to a police department in Massachusetts to a Native American tribe in Washington."[24] He also, as *Wired* summarized, created "the digital underground's malware of choice—the Microsoft Office of online fraud."[25] While Bogachev was after money, Russian intelligence was able to piggyback off Bogachev's efforts and search the same computers he had accessed for information. Austin Berglas, former assistant special agent in charge of cyberinvestigations at the FBI, explained that hackers such as Bogachev are "moonlighters … doing the bidding of Russian intelligence services, whether economic espionage or straight-up espionage."[26]

Russian intelligence and cybercriminals were behind the hack of Yahoo

In March 2017, the Department of Justice indicted four Russian nationals, including two Russian intelligence officers, for hacking into Yahoo's systems.[27] This was the first time the United States has indicted Russian government officials. They sought "to steal information from about at least *(sic)* 500 million Yahoo accounts and then used some of that stolen information to obtain unauthorized access to the contents of accounts at Yahoo, Google and other webmail providers, including accounts of Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies." U.S. law enforcement had initially indicted the suspected Russian hacker, Alexsey Belan, in 2012, but he escaped to Russia. Instead of handing him over to face trial in the United States, Russian intelligence used him for the hack into Yahoo. In 2014, The Daily Beast explained, "The hack had a substantial economic impact. Verizon ended up paying $350 million less to purchase Yahoo than it initially offered because the hack damaged its brand so much."[28] The indictment outlines that in addition to diplomatic targets, the Russian hackers got into accounts of a Nevada gaming official, a senior officer at a major U.S. airline, and an employee at a U.S. financial institution, among others.

A slew of Russian cybercriminals nabbed on vacation

Because Russia shields Russian cybercriminals, the Department of Justice has made a point of targeting Russian cybercriminals when they leave Russia. Between 2010 and 2016, an average of two Russian cybercriminals were extradited to the United States each year. As of this past August, the United States had arrested or indicted seven Russians for alleged U.S. cybercrimes in 2017 alone, marking a record high.[29] These include:

- **Pyotr Levashov,** allegedly "[o]ne of the world's most notorious criminal spammers," who created a series of botnets that enabled him to send more than one billion emails per day. He was arrested in Spain and is awaiting extradition.[30]
- **Evgeny Nikulin,** who is accused of hacking into LinkedIn and Dropbox, affecting tens of millions of users. He was arrested in Prague and is awaiting extradition.[31]
- **Alexander Vinnik,** who is alleged to have "helped to launder criminal proceeds from syndicates around the world" by creating a bitcoin exchange. He was arrested in Greece, and a Greek court recently cleared him for extradition to the United States where he will be brought to trial.[32]

- **Yury Martyshev,** who allegedly ran a "counter antivirus service" where cybercriminals could test the malware they developed. He was arrested and extradited from Latvia and is awaiting trial in Virginia.[33]
- **Stanislav Lisov,** who is alleged to have stolen information on bank clients, resulting in nearly $1 million in losses in the United States. He was arrested at the Barcelona airport and is awaiting extradition.[34]

Kremlin uses Russian private sector firms to infiltrate U.S. government systems

In October, *The Wall Street Journal* reported that the Russian government had stolen highly classified details from an NSA contractor's home computer. The stolen information included details on how the United States protects itself from cyberattacks and how they access foreign computer networks.[35] It appears that hackers were able to target the files via the contractor's use of antivirus software made by the Russian cybersecurity firm Kaspersky Lab. According to the *Journal,* the breach occurred in 2015 but was not discovered until the spring of 2016. Shortly before this report, the DHS had ordered that all software made by Kaspersky Lab be removed from government computer systems amid growing concerns that the company might have ties to Russian intelligence agencies—ties the FBI has long been trying to uncover and that Kaspersky denies.[36] *The New York Times* also reported that Israeli intelligence officers discovered Russian government hackers using Kaspersky Lab antivirus software around the world as an "improvised search tool" to hunt for classified U.S. government programs.[37] Their antivirus software is used by 400 million people globally, including, until recently, by the U.S. Departments of State, Defense, Energy, Justice, and Treasury, as well as the Army, Navy, and Air Force. As the Center for Strategic and International Studies outlined in its 2016 report, the "Kremlin Playbook," Moscow frequently uses Russian businesses and its network of oligarchs, whose vast wealth is largely preserved by their submission to the Kremlin, to infiltrate and influence democratic societies.

Russia hacked the Olympics

Following the Summer Olympics in Rio de Janeiro last year, the World Anti-Doping Agency (WADA) confirmed that it had been hacked and confidential information on more than 40 Olympic athletes was revealed.[38] The same hackers who targeted the Democratic National Committee (DNC), the Russian hacking group APT28—also known as Fancy Bear or Pawn Storm—claimed responsibility for the hack.

They are believed to be part of the GRU, the military intelligence agency of the Kremlin. They selectively released the private medical information of American athletes, such as gold medal gymnast Simone Biles, who has ADHD. These hacks were seen as retaliation against WADA, which had recommended banning all Russian athletes from the Olympics in Rio after it was revealed that Russia conducted a massive state-sponsored doping campaign during the Sochi Winter Olympics.[39] WADA just ruled that Russia failed to take steps to address doping and remains "non-compliant" with its standards. The International Olympic Committee will decide whether to ban Russian athletes from the 2018 Winter Olympics in South Korea at a meeting in December.[40]

Russia's continuing espionage efforts against the United States

Russia is expanding its effort to recruit spies and agents of influence in the United States. In a report on Russian espionage, *Politico* assessed, "After neglecting the Russian threat for a decade, the U.S. was caught flat-footed by Moscow's election operation. Now, officials are scrambling to figure out how to contain a sophisticated intelligence network that's festered and strengthened at home after years' worth of inattention … U.S. intelligence officials say Moscow's espionage ground game is growing stronger and more brazen than ever."[41]

Russia is engaged in an aggressive cyberespionage campaign against the U.S. Government

Russia has prioritized the United States as a top espionage target, devoting considerable resources to spying on the United States. While it is no surprise that Russia and the United States spy on each other, the Kremlin's actions clearly demonstrate that Russia does not see the United States in any way as a partner.

Russia targeting the U.S. intelligence community

A major priority for Russian intelligence is countering the efforts of U.S. intelligence. American officials suspect Russia of being linked to a number of recent high-profile security breaches, according to *The New York Times*.[42] For instance, Russia is the prime suspect behind the hacking and exfiltration of a trove of documents from the Central Intelligence Agency's (CIA) Center for Cyber Intelligence.[43] The documents were published by WikiLeaks and exposed a vast array of the CIA's hacking techniques and capabilities.[44] The NSA experienced a massive security breach by a group known as the "shadow brokers," which released top secret NSA code that it developed for offensive cyberattack operations. The release of this code is suspected of providing the basis for the recent spate of ransomware attacks.[45] While it remains unknown who was behind the security breech, *The New York Times* reported that "American officials strong belief is that it is a Russian operation."[46]

Russia targeting U.S. military forces

As documented in a *Politico* investigation, Russian state actors have targeted U.S. service members on Facebook to gather intelligence and have targeted Pentagon-employee Twitter accounts with phishing attacks. Russia also reportedly targeted the personal smart phones of deployed NATO forces. They are attempting to acquire sensitive information, such as force numbers and personal information about these forces, and potentially have the ability to sow confusion in a crisis by sending out fake orders or information.[47] Russia is seeking "to hobble the ability of the [U.S.] armed forces to clearly assess Putin's intentions and effectively counter future Russian aggression."[48]

Russia targeting U.S. diplomacy

In November 2014, Russian hackers breached the State Department's unclassified computer system in what former NSA Deputy Director Richard Ledgett recently described as "hand-to-hand combat" and a "new level of interaction between a cyberattacker and a defender."[49]

Russia using the internet to compromise and recruit agents of influence in the United States

As noted in the CAP report "War by Other Means," what makes the new online information landscape so troubling is that Russia has been able to expand its espionage efforts against the United States with little consequence.[50] 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. Once compromising information—what the Russians call kompromat—is obtained, Russian intelligence agents can use this as leverage over individuals.

- **Russia intelligence targets sent malicious links through social media.** Citing information from the cybersecurity firm SecureWorks, security studies Professor Thomas Rid found that, in a period of 14 months, the GRU sent "19,300 malicious links, targeting around 6,730 individuals."[51] For Russia, this likely yielded a trove 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.

- **Russia creates fake and anonymous online honeypots.** A common intelligence tactic to gain leverage over an intelligence target is to seek to capture them in a sexually compromising situation. Andrew Weisburd, J.M. Berger, and Clint Watts, explain, "In addition to phishing and cracking attacks, these hackers are aided by honeypots, a Cold War term of art referring to an espionage operative who sexually seduced or compromised targets. Today's honeypots … often appear as friends on social media sites, sending direct messages to their targets to lower their defenses through social engineering. After winning trust, honeypots have been observed … attempting to compromise the target with sexual exchanges, and most perilously, inducing targets to click on malicious links or download attachments infected with malware."[52]

- **Russia used hotel Wi-Fi to spy on guests.** In August, the security firm FireEye released a report detailing a Russian espionage campaign believed to be carried out by the group APT28. It utilized hotel Wi-Fi networks in at least eight countries in Europe and the Middle East in order to spy on guests and gain access to personal data.[53] As summarized in *Wired*, APT28 utilized a new technique to gain access to guest information that "doesn't even require users to actively type" their credentials "when signed onto the hotel network."[54]

Russia's escalating harassment of U.S. diplomats

Russian harassment and surveillance of diplomatic staff increased significantly following Russia's annexation of Crimea in 2014. Russian security services are suspected of breaking into the homes of American diplomats in Russia, slashing tires, and even reportedly killing the U.S. defense attaché's dog.[55] Furthermore, in June 2016, a U.S. intelligence officer working in the U.S. embassy in Moscow was brutally assaulted outside the embassy after having lost his Russian tail. His shoulder was broken and he was evacuated from the embassy. Former CIA Director John Brennan told Congress in May 2017 that "the continued mistreatment and harassment of U.S. diplomats was intolerable."[56] As *The Washington Post* reported in 2016, Russian intelligence and security services "have been waging a campaign of harassment and intimidation against U.S. diplomats, embassy staff, and their families in Moscow" and across Europe. This prompted former Secretary of State John Kerry to ask Putin directly to put an end to the behavior[57] and resulted in the June 2016 eviction of two Russians from the United States. However, a U.S. intelligence official told *Politico*, "They are far more aggressive on counterintelligence issues in Russia than we are here."[58]

Russia suspected of assassinating enemies abroad, including in the United States

Over the past decade, there have been a series of mysterious deaths in the United Kingdom and in the United States. Since the 2016 U.S. election, at least seven Russian diplomats, a senior former intelligence official, and a dissident politician in Ukraine have been killed.[59] Some were murdered, while some appeared to die of natural causes—both in mysterious circumstances and some not. As former FBI agent Clint Watts told the Senate intelligence committee in March, "[F]ollow the trail of dead Russians." As Watts explained, "[I]f you look over the past year, really year and a half, you've seen a string of senior Russian officials that have died, some of them obviously of natural causes but some of them under suspicious circumstances."[60]

- **U.S. Intelligence agencies link 14 suspicious deaths in the United Kingdom to Russia.** In a blockbuster five-part series, a BuzzFeed investigation uncovered a string of mysterious deaths in the United Kingdom. Its investigation concluded that Russia assassinated its enemies, including Russian dissidents and emigres, but also a British journalist as well as a U.K. intelligence official, whose body was found in a North Face bag in his bathtub. BuzzFeed assessed, "The story of this ring of death illuminates one of the most disturbing geopolitical trends of our time—the use of assassinations by Russia's secret services and powerful mafia groups to wipe out opponents around the globe—and the failure of British authorities to confront it … The intelligence pointing to a campaign of targeted killings in Britain comes amid mounting international concern that the Kremlin is brazenly interfering in the West."[61]

- **FBI agents reportedly believe Russia behind an assassination in Washington, D.C., hotel.** BuzzFeed discovered that "Vladimir Putin's former media czar was murdered in Washington, D.C., on the eve of a planned meeting with the U.S. Justice Department, according to two FBI agents ... Mikhail Lesin's battered body was discovered in his Dupont Circle [Washington, D.C.] hotel room on the morning of Nov. 5, 2015, with blunt-force injuries to the head, neck, and torso." The death was deemed an accident, but BuzzFeed reports that "two FBI agents—as well as a third agent and a serving US intelligence officer—said Lesin was actually bludgeoned to death … 'Lesin was beaten to death ... there isn't a single person inside the bureau who believes this guy got drunk, fell down, and died. Everyone thinks he was whacked and that Putin or the Kremlin were behind it.'"[62] Murdering an individual in the United States is not acceptable and would represent a significant escalation in Russian hostility against the United States.

Russian organized crime is used as a tool of the Kremlin

Just as Russian hackers are often used as tools of the Russian state, so are Russian organized criminals. Mark Galeotti of the Institute of International Relations Prague explains in *Foreign Policy*, "[Russia is] increasingly turning to organized crime groups as proxies, intelligence assets, and sometimes even as hired killers. Welcome to the modern age of hybrid war, when even crime has been weaponized."[63] In a report for the European Council on Foreign Relations, Galeotti explains further that there is "growing evidence of connections between such [Russian-based] criminal networks and the Kremlin's state security apparatus, notably the Foreign Intelligence Service (SVR), military intelligence (GRU), and the Federal Security Service (FSB) … We are seeing more and more cases, especially in Europe, where local counterintelligence services believe gangsters are acting as occasional Russian assets. Some work on behalf of the Russia state willingly. In other cases, these criminals have been turned into assets without their knowledge, thinking they are simply doing a service for a Russian gang. And yet for others, they are made an offer they can't refuse."[64] Brian Whitmore, a Russia-watcher for Radio Free Europe/Radio Liberty, notes, "Moscow relied heavily on local organized crime structures in its support for separatist movements in Transdniester, Abkhazia, South Ossetia, and Donbas."[65]

Russia has also provided a safe haven for Russian organized crime bosses. For instance, in April 2013, an FBI investigation led to the indictment of more than 30 people—including a man who ABC News described as "one of the world's most notorious Russian mafia bosses," Alimzhan Tokhtakhounov—for allegedly operating a criminal gambling and money laundering operation out of unit 63A in Trump Tower, just three floors below Donald Trump's residence.[66] Tokhtakhounov was the only one to escape, prompting Interpol to issue a "red notice" for his arrest. Yet, seven months later, Tokhtakhounov was photographed on the red carpet at Trump's 2013 Miss Universe pageant in Moscow.[67]

ProPublica conducted an extensive report on Spain's efforts to counter Russian organized crime. It found, "The mafias' ties to the Russian government, and particularly to the security services, have led Spanish officials to fear for their national security as well as law and order."[68] A senior Spanish police official told ProPublica, "[T]here is always the shadow of intelligence services behind [Russian] organized crime." Spain found that Russian organized criminal groups were connected "to murders, kidnapping, extortion, robbery and drug and arms trafficking." According to court documents reviewed by ProPublica, one key crime boss, Gennady Petrov,

was even connected to the alleged black-market sales of Russian military helicopters and MiG fighter jets to Africa. Furthermore, the Spanish police recorded intercepts of "Petrov's contacts with a Russian deputy prime minister and at least five other cabinet ministers, as well as legislators, oligarchs and bankers, investigative documents show. And his influence was remarkably steady, given the volatility of the Putin regime." Petrov has denied the charges against him. As Galeotti assessed, "[O]rganised crime groups … are likely to become an even greater problem as Russian's campaign to undermine Western unity and effectiveness continues."[69]

Russia is probing ways to attack America

As Russia's economy boomed from high energy prices, Russia significantly increased investments to modernize its military. But understanding its weakened military position relative to the Soviet Union's position with the United States, Russia has sought to find asymmetric ways of attacking America that could level the military playing field. Russia is probing critical U.S. infrastructure and examining ways in which it could strike at it. Most recently, Ciaran Martin, the head of the U.K. Cyber Security Centre, disclosed that Russian hackers had conducted "attacks on the UK media, telecommunications and energy sectors."[70] While much of this espionage is not unusual for adversaries, it also signals that Russia is looking for nonkinetic ways to potentially retaliate against the United States and its allies that fall short of escalating toward a military conflict.

Russia is targeting U.S. nuclear power plants

At the end of June, the FBI and DHS issued a joint report to industrial firms disclosing a series of hacking attempts—some of which were successful—targeted at the nuclear and energy sectors, including at least one on a nuclear power plant in Kansas.[71] The report concluded that "hackers appeared determined to map out computer networks for future attacks."[72]

According to U.S. government officials, Russian government hackers were responsible. The Russian hackers had gained access to the business networks of U.S. nuclear power companies.[73] While they were not able to breach the operations systems controlling the power plants, as *The Washington Post* noted, the attacks "could be a sign that Russia is seeking to lay the groundwork for more damaging hacks."[74] These latest attacks are not the first time the Russian government has targeted U.S. infrastructure either: In 2014, they conducted a similar campaign targeting U.S. industrial control systems.[75] These kinds of attacks are not confined to the U.S.; the same hackers have also targeted similar energy systems in Ireland and Turkey[76] and were responsible for the most recent attack on Ukraine's energy system which "briefly shut down one-fifth of the electric power generated in Kiev."[77]

Russia is targeting the U.S. financial sector

Following the imposition of sanctions against Russia for its illegal occupation of Crimea, Russia is suspected of retaliating against the U.S. financial industry by hacking into JPMorgan Chase and another U.S. bank.[78] In 2014, the FBI arrested a Russian spy ring in New York. One of the Russian agents, was operating under cover as an employee of Vnesheconombank, a sanctioned Russian bank. According to the FBI's indictment, these Russian intelligence figures sought information on high-frequency trading systems.[79] In 2010, the Nasdaq stock exchange discovered a malicious cyberattack code, and Russia was seen as the likely culprit. According to *Wired*, in 2014, the Warsaw Stock Exchange was hacked by a Russian group false-flagging as "cyber-jihadists."[80] Cameron Colquhoun of the firm Neon Century wrote in *Wired,* "The erroneous and uncontrollable behaviour of trading algorithms—known as flash crashes—are regular occurrences in many stock markets. Critically, there are few human stockbrokers left, leaving the financial world with no backup if the markets were manipulated or wiped."[81]

Russia is targeting U.S. communication infrastructure

One way Russia could significantly retaliate against the United States is to take down U.S. communications networks and infrastructure. Nearly every aspect of U.S. society—its economy, its energy and power sectors, its military—is dependent on the viability of the communications network, which would make such an attack devastating.

Russian operatives targeting U.S. fiber-optic cables and telecommunications infrastructure

Politico described U.S. officials seeing an increase in alarming behavior in the United States throughout 2016 on the part of Russian diplomats who are "widely assumed to be intelligence operatives."[82] Russian diplomats, whose travel is closely monitored by the State Department, repeatedly went missing for periods of time, often ending up in seemingly random places in the United States. Some were found "to be lingering where underground fiber-optic cables tend to run," and others were found driving in circles. This behavior "has led intelligence officials to conclude that the Kremlin is waging a quiet effort to map

the United States' telecommunications infrastructure, perhaps preparing for an opportunity to disrupt it." Additionally, *The New York Times* reported in 2015 that U.S. officials fear that, in the midst of a conflict, Russia may try to sever undersea cables at the hardest to reach areas deep in the ocean.[83]

U.S. satellite and communication systems are targets

As the director of National Intelligence, Dan Coats testified in May before the Senate Select Committee on Intelligence that Russia would seek to "offset any U.S. military advantage from … space systems and are increasing increasingly considering attacks against satellite systems as part of their future warfare doctrine."[84]

Russia is testing and working to undermine our ability to respond to disasters

On September 11, 2014, 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 Kremlin-connected 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.[85] These complex efforts are designed to sow public distrust of the U.S. media and U.S. government institutions.

Russia continues to intervene in American politics

Russia did not stop its aggressive intervention in American politics after the 2016 election. Russia continues to wage an aggressive influence campaign, utilizing U.S. social media platforms and troll farms as well as Russian-media news outlets. As Ben Nimmo of the Digital Forensics Lab of the Atlantic Council assessed, "They [the Russians] haven't stood still since 2016."[86] Laura Rosenberger of the German Marshall Fund observed, Russia is "potentially laying the groundwork for what they're going to do in 2018 and 2020."[87]

Russian troll farms are still at work

In December, the now infamous Internet Research Agency reportedly shut its doors. But CAPAF's Moscow Project uncovered through analyzing Russian corporate records that it likely has reformed under a new name: Glavset. CAPAF's Diana Pilipenko told *Wired*, "It's there … It's alive and well and operating."[88] She added, "If Facebook has only identified ads purchased by one of these companies, there needs to be an immediate investigation into activity by everything in this 'Kremlebot' empire … This may just be the tip of the iceberg."

Russia continues to operate fraudulent accounts on U.S. social media platforms

ThinkProgress examined accounts identified by Twitter as fraudulent and found that "the accounts in question reveal that at least three of the suspended, Russia-linked Twitter accounts link back to multiple Facebook pages—pages that remain live even after last week's congressional hearings."[89] As Andrew Weisburd and Brett Schafer of the German Marshall Fund's Hamilton 68 project assess, "No longer is advanced tradecraft required to execute a successful influence operation; now, basic cultural and linguistic skills, along with an understanding of trending algorithms, is all that is needed for Kremlin-oriented accounts to insinuate themselves into more organic social networks, including in the United States."[90]

Bots continue to amplify and harass

A report from the Virginia Education Association found that, during the Virginia gubernatorial election, bots were amplifying a controversy over an advertisement. Timothy Chambers, one of the researchers of the report, told *The Washington Post*, "We are seeing the same exact techniques that attempted to skew the social media conversation and affect hashtags trending and search results that we saw in the [presidential] election."[91] Bloomberg reported that a "pro-Kremlin cyborg site … averages a rate of more than 220 tweets a day, including memes about McCain in the week after the Charlottesville unrest."[92]

Kremlin pushing anti-American conspiracy theories

Russia released a video in November 2017 that it claimed proved that American forces in Syria were allowing Islamic State fighters to escape from surrounded cities. It was later revealed that the Russian video was a fake. Moscow was using images from a video game trailer and clips from the Iraqi Ministry of Defense. As The Washington Post's Christian Caryl assessed, "[This] is but one example of how Moscow's state-sponsored lie machine keeps cruising along even as its operations are being unveiled."[93] The spokeswoman for the Russian foreign ministry, Maria Zakharova, even claimed that a fake photograph of Osama bin Laden being hosted at the White House was true. Putin himself pushed conspiracy theories that the United States is preparing for biological warfare, saying that the United States has been collecting tissue samples of Russians, asking "Why are they going to different ethnic groups and to people living in different geographical locations across Russia?" Adding, "why are they doing this?"[94]

Russia seeking to sow division; stoke the far right

The German Marshall Fund's Hamilton 68 project has highlighted the continuing efforts of Russia to influence American politics on Twitter. Highlighting the themes of Russian influence operations on Twitter, they note that the Russians are heavily enmeshed in supporting the alt-right. On November 6, they assessed, "Between October 21 and November 3, we examined 121 unique articles that were among the top URLs shared by Kremlin-oriented Twitter accounts. Of those URLs, 30 percent were anti-Hillary Clinton, 11 percent were anti-Robert Mueller, 7 percent were anti-Barack Obama, and 4 percent were anti-Tony Podesta (several URLs attacked a combination of or all of the above figures)."[95] Kremlin-messaging is heavily symbiotic with much of the alt-right messaging.

Russia continues to use its official media outlets, such as RT and Sputnik, to amplify stories and launder fake information

RT and Sputnik clearly serve as propaganda arms of the Russian state and have, therefore, been required to register as foreign agents under the Foreign Agents Registration Act (FARA); Russia has said it will challenge the decision in court.[96] RT uses the tagline "Question More" to justify pushing conspiracy theories and sowing doubt in Western state institutions. Because Russia 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, and had Green Party candidate Jill Stein seated at the same table at the RT gala as Michael Flynn, President Trump's short-lived national security adviser.[97] 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.

Russia aggressively intervened in European elections in 2017

Russia seeks to sow doubt and discredit the American and European democratic systems and, to do so, it seeks to amplify fringe and extremist views that often cast doubt on democratic institutions or espouse conspiracy theories. Russia extensively intervened in European elections throughout 2017.

- **Germany:** During the German elections in September, Russia amplified anti-immigrant sentiment and amplified messages favorable to the far-right Alternative for Germany (AfD), which had its best ever showing. In 2015, Russia also hacked into and stole data from the German Bundestag.[98]

- **France:** Russia hacked the campaign of Emmanuel Macron and attempted to leak damaging information just a few days before the election. Russia reportedly financed the campaign of Marine Le Pen of the far-right National Front,[99] who met with Putin in Moscow just a month before the French election.[100]

- **The Netherlands:** Russian disinformation and propaganda arms heavily targeted the Netherlands before the March election, spreading fake news and amplifying anti-immigrant sentiments.[101]

Russia provides backing to secessionists in European Union and United States

As part of their efforts to undermine the European Union, as well as the United States, Russia has been supporting secessionist movements. Some of these movements have genuine local support; others are clearly manufactured efforts.

- **Catalan independence:** On November 10, the Spanish government confirmed that Russian hackers had been interfering in the crisis in Catalonia. The Spanish defense minister, María Dolores de Cospedal, revealed, "The government has corroborated the fact that many messages and operations that were seen via social networks come from Russian territory."[102]

- **Russia supports fringe secessionist movements in the United States, such as the Texas Nationalist Movement and Yes California.** The purported leader of Yes California actually lives in Russia and opened an "embassy" in Moscow.[103] *Politico* also reported that Russia has also sought to amplify Texan secessionists, bringing them to a far-right conference in Russia and using RT, Sputnik, and Russian-linked bots to amplify their reach.[104]

Russia providing backing to extremist European political parties and groups

As detailed extensively in CAP report "Russia's 5th Column," Russia has been providing support to far-right parties across Europe.[105] Such support has come in various forms, ranging from "elevating the profile of European far-right leaders to disinformation, propaganda, alleged illicit financing, and covert influence operations." In exchange, these parties have provided Russia with international support and have undertaken actions favorable to Russia's objectives, such as supporting the lifting of sanctions against Russia and blaming the European Union and NATO for the crisis in Ukraine.

Russia undermining international law and treaties

Russia has violated key tenets of international law through its military invasions and annexation of neighboring countries, including Georgia and Ukraine. Russia is also not in compliance with a key arms control treaty.

Russia violated international law and its treaty commitments by illegally seizing and occupying Ukrainian territory

Since 2014, Ukraine and Russia have been in a de facto war, as Russia illegally occupied and seized the Ukrainian territory of Crimea and initiated a separatist war using proxies in eastern Ukraine. As a result, Ukraine has borne the brunt of Russia's cyber and espionage capabilities. This is a violation of the U.N. Charter and the Helsinki Final Act. Russia broke a key principle of post-World War II international order—that stronger powers will not seize territory and redraw borders. It is also a clear violation of the 1994 Budapest Memorandum, in which Russia pledged to "to respect the independence and sovereignty and the existing borders of Ukraine."[106]

Russia engaged in a proxy war in eastern Ukraine

Russia is waging a separatist war to undercut the new Ukrainian government. Russia established a proxy force in eastern Ukraine—arming, funding, and manning these forces. In summer 2014, when the Ukrainian military was routing these forces, Russia invaded eastern Ukraine with its regular forces and drove back the Ukrainian military. Russia's proxy forces are also responsible for the downing of MH17, killing 270 passengers.[107]

Ukraine a Russian "test lab for cyberwar"

As *Wired* described it, Ukraine has been "Russia's test lab for cyberwar."[108] In December 2015 and 2016, Russian-connected hackers are alleged to have twice caused blackouts to a quarter of a million Ukrainians in the middle of the Ukrainian winter. In December 2016, Ukraine's president Petro Poroshenko announced that, in just the previous two months, there had been 6,500 cyberattacks against 36 Ukrainian targets. As *Wired* assessed, the "digital blitzkrieg that has pummeled Ukraine for the past three years … [is] a sustained cyber assault unlike any the world has ever seen. A hacker army has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, energy. Wave after wave of intrusions have deleted data, destroyed computers, and in some cases paralyzed organizations' most basic functions." As John Hultquist of cybersecurity firm FireEye concluded, "We've seen this actor show a capability to turn out the lights and an interest in U.S. systems."

Russia likely behind a slew of assassinations and terrorist bombings in Ukraine

Ukraine has been rocked by a continuous wave of assassinations. These include a slew of bombings and shootings, sometimes in broad daylight, targeting Russian dissident politicians, Ukrainian military officers, and political figures.[109]

Human rights abuses in Crimea

A U.N. human rights report found "grave human rights violations, such as arbitrary arrests and detentions, enforced disappearances, ill-treatment and torture, and at least one extra-judicial execution." In particular, Russia has arrested leaders of the Crimean Tatars, a minority group in Crimea, that have spoken out against the illegal Russian occupation. The U.N. report found that Russia "has infringed on the civil, political, and cultural rights of Crimean Tatars."[110]

Russia in violation of the INF Treaty

Russia is in violation of the Intermediate-Range Nuclear Forces Treaty, which bans missiles with ranges between 500 kilometers and 5,500 kilometers. In 2014, the United States accused Russia of being in violation of the treaty. The United States and NATO are pressuring Russia to return to compliance with the treaty, as their failure to do so could spark a dangerous arms race. While Russia is in violation of the INF treaty, it has remained compliant with the New START treaty.[111]

Russian military operating dangerously and provocatively

Russia's military posture toward the United States and NATO is adversarial. As tensions have increased, especially after Russia's illegal annexation of Crimea in 2014, there have been an increasing number of dangerous and provocative air and sea incidents instigated by Russian military forces. Furthermore, Russia's military posture and military exercises are often directed against the United States and its allies, just as those of the United States and NATO are often directed against Russia. This further demonstrates that both Russia and NATO operate militarily as strategic adversaries. Reflecting this reality, the commander of U.S. European Command and the supreme allied commander of Europe, General Curtis Scaparrotti, testified to Congress in early May, saying, "EUCOM has shifted its focus from security cooperation and engagement to deterrence and defense … we are returning to our historic role as a warfighting command."[112]

Dangerous incidents between U.S. and Russian planes and ships are increasing

Fox reported that there were more than 35 encounters between U.S. and Russian planes and ships in June.[113] On June 21, 2016, a Russian fighter jet, a Su-27 Flanker, flew within 5 feet of a U.S. Air Force reconnaissance plane in international waters over the Baltic Sea. U.S. European Command called the Russia's actions "provocative" and "unsafe."[114]

- **Russia violating airspace of NATO members as well as neutral states.** Russian fighter jets have repeatedly violated the air space of Baltic and Nordic countries. Sweden summoned Russia's ambassador following a Russian fighter jet flying very close to a Swedish reconnaissance plane in international airspace over the Baltic.[115] On June 21, a Russian plane flying with the Russian defense minister was flying with its transponders off, prompting a response from Polish NATO planes, which in turn prompted a Russian fighter jet to respond as well.[116] Defense Minister for Finland Jussi Niinistö explained, "We take these incidents seriously … Having two suspected violations on the same day is exceptional."

- **Russia operating recklessly, flying with transponders off.** The chairman of NATO's military command, General Petr Pavel, explained, "We are mostly witnessing what we call unprofessional behavior in the airspace. When these rules are broken the chance of getting into an incident is pretty close."[117]

Russia's military orientating to combat and counter the United States and NATO

Russia has modernized its military and has built up its capabilities to counter NATO forces. Russia has turned the Russian territory of Kaliningrad, an enclave on the Baltic between Poland and Lithuania, into a military battle station. Russia has deployed nuclear capable Iskander-M missiles that have a range of 500 kilometers, which means it can target NATO facilities as well as a number of major NATO cities, such as Berlin.[118] Moscow has also deployed its advanced S-400 anti-aircraft system and the P-800 Oniks, a supersonic, anti-ship cruise missile. These armaments would hinder any NATO effort to support the Baltic states in a conflict and pose a threat to alliance activities in the Baltic Sea. According to Sergey Sukhankin in a commentary for the European Council on Foreign Relations, "The intensity with which Russia has militarised the oblast in recent years has dispelled any remaining illusions about Kaliningrad becoming a bridge of cooperation with the West."[119] Russia is also conducting military exercises and war games designed to counter NATO forces. The recent Zapad exercise in Belarus, as Chatham House characterized, "[L]ooked like a dress rehearsal for defending against a NATO intervention. This is what Russia wants the West to believe is the Kremlin's understanding of what a conventional war between Russia and NATO forces would look like."[120]

Russia acting against U.S. interests and international stability worldwide

A key objective of Russian foreign policy is to undermine U.S. interests and U.S. global leadership.

Syria

Russia militarily intervened on behalf of the regime of Bashar Al-Assad, which had used chemical weapons and carried out war crimes against its own citizens. Russia's intervention turned the tide of the conflict,[121] contributing to a massive refugee and humanitarian crisis and assuring the survival of the brutal regime. Former head of U.S. European Command and the supreme allied commander of Europe, General Philip Breedlove, said Russia and Assad were "deliberately weaponising migration in an attempt to overwhelm European structures and break European resolve."[122] Furthermore, Russia's intervention has done little to counter the Islamic State, which was the major focus of the U.S.-led coalition's military intervention.[123]

North Korea

Russia is undercutting the sanctions regime. *The Washington Post* reports that Russian smugglers are shipping fuel and other vital goods that will help soften the blow of sanctions.[124] The increase in shipping traffic even prompted the creation of a dedicated ferry line between the North Korea ports of Rajin and Vladivostok early the summer. Russia also continues to use cheap North Korean laborers and has worked with China to water down the U.N. sanctions against North Korea.[125]

The Balkans

Russian efforts in the Balkans seek to erode democratic institutions and turn these countries away from the European Union and the United States. For instance, Russia is suspected of being involved in the recent failed coup in Montenegro and for supporting radical leaders in the region.[126]

Venezuela

Russia is an ally and backer of the Maduro regime in Venezuela and is providing it with vital "cash and credit," which is essentially keeping the regime afloat.[127]

Afghanistan

According to the U.S. military and the U.S. State Department, Russia has been providing arms to the Taliban, which the U.S.-led NATO coalition is combatting.[128] Reuters reported that a senior U.S. official indicated "the supply of weapons has accelerated in the past 18 months."[129]

Recommendations

The post-Cold War strategy of seeking to integrate Russia into the liberal global order is no longer operable. Russia under 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. As such, it is critical that the Trump administration and congressional lawmakers take action to both deter Russia's aggressive behavior and to protect the United States and its allies from further attacks.

After 9/11, knowing the threat from terrorism would be all-consuming, Congress established the U.S. Department of Homeland Security and implemented a whole host of reforms to improve the U.S. government's defenses. After the voting issues surrounding the 2000 election, Congress passed the Help America Vote Act in 2002, which allocated $3.65 billion to improve America's voting systems.[130] Yet, currently, little is being done despite Russia's intervention in the 2016 election. Congress and the White House have not acted to protect America from the clear threat posed by Russia. The following are actions and approaches that the Trump administration and Congress should take.

The White House and Congress must stop efforts to appease Moscow

The first step in addressing the challenge posed by Russia's hostile actions is to stop pretending that they are not occurring. President Trump continues to cast doubt on the assessments of the U.S. intelligence community and, along with his secretary of state, resist efforts to address them. The Republican-led Congress has not called out the White House for its efforts to appease the Kremlin nor has it prioritized this challenge. The muddled messages from Washington are likely interpreted as a green light for Russia to advance its efforts. Instead, the White House and Congress must send a clear message to Russia that efforts to undermine America and its allies will be countered strongly.

Protect America's elections from foreign cyberattacks

According to a report by CAP's Michael Sozan, protecting America's election system could cost as little as $1.25 billion over a 10-year period—a fraction of previous election infrastructure reforms.[131] The price tag for securing America's elections would require just $1 billion to update outdated voting machines; $5 million per year to conduct threat assessments for voter registration databases; and $20 million per year to conduct nationwide risk-limiting audits for federal elections. There is bipartisan legislation in the Senate, introduced by Sens. Amy Klobuchar (D-MN) and Lindsey Graham (R-SC), and the House of Representatives, introduced by Reps. Jim Langevin (D-RI) and Mark Meadows (R-NC), that would take major steps to address the threat. Yet Majority Leader McConnell and Speaker Ryan have currently blocked this legislation from even receiving a vote.

Aggressively implement U.S. sanctions against Russia

Congress must ensure that the Trump administration aggressively implements the new sanctions legislation, which could cause a severe blow to the Russian energy and defense sectors. For instance, reports that Saudi Arabia has agreed to purchase a Russian air defense system for an estimate of $2 billion dollars could make the Saudis subject to U.S. sanctions. Should Saudi Arabia follow through on this deal, the United States should be prepared to levy sanctions against the Saudi government.[132]

Bolster U.S. intelligence and cyberdefense capabilities to better cope with Russia

The United States needs to bolster the intelligence resources and assets devoted to monitoring Russia, especially in countering Russian intelligence efforts against the United States and its allies. 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. Congress must properly resource these efforts and ensure that investigations into Russian intervention continue. Additionally, the United States needs to take urgent steps to ensure the security of its cyberweapons and to combat Russian cybercriminals.

Stand up for democracy and human rights

Combating the Kremlin is fundamentally about the highest levels of the U.S. government standing up in support of freedom and democracy around the world. Unfortunately, the Trump administration not only has failed to speak up for democracy and human rights but has also actively sought to undermine these values and what America stands for. It is bending over backward to accommodate and offer support to authoritarian governments and strongman rulers.[133] Moreover, Trump's attack on the press; Secretary Tillerson's unwillingness to allow the press to travel with him; 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.[134] When the leader of the free world no longer values democracy, these principles are weakened worldwide.

Hold social media companies accountable

Russian operatives and troll farms are exploiting their access to U.S. social media to conduct information operations on their platforms. These social media companies are not doing enough to stop Russian efforts. Congress must hold these companies accountable, including through regulations and legislation that ensure these platforms are transparent to their users, protect user information and data, and are not serving as vehicles for public manipulation and disinformation. Congress should immediately move to pass the "Honest Ads Act," which would require online political advertising on social media companies to have a similar level of transparency as ads broadcast by television and radio stations.[133]

The United States should take action against money laundering

The Unites States should introduce policies aimed at curtailing systemic money laundering through anonymous purchases of domestic real estate. The banking and financial services industry can be used as a model, as they are mandated to report any suspicious transactions to law enforcement and have in place anti-money laundering controls, which have proven effective in detecting and preventing the use of lending institutions to facilitate the laundering of ill-gotten gains. The Financial Crimes Enforcement Network (FinCEN) of the Treasury Department has already made steps in the right direction with the introduction of the geographic targeting orders that have temporarily required U.S. title

insurance companies to identify the ultimate beneficiaries behind shell companies used to pay "all cash" for high-end residential real estate in several U.S. risk-prone jurisdictions, including New York and Miami.[134] What's more, the United States should take steps to crack down on the use of shell companies as vehicles for money laundering, particularly in the state of Delaware, where limited reporting requirements allow individuals, including foreign nationals, to set up anonymous shell companies without listing directors or shareholders. The intrinsic anonymity of shell companies makes them a favored means by which to facilitate the laundering of money on a large scale.

Block Secretary Tillerson's efforts to undermine U.S. diplomacy

To counter Russian efforts around the world, the United States needs a robust State Department and diplomatic corps to get the rest of the world to follow the lead of the United States and adopt policies that isolate Russia. Congress should use all available leverage points it has to block Secretary Tillerson's efforts to downsize and deconstruct the State Department.[135] For instance, Congress can indefinitely hold all arms sales until the secretary of state properly staffs his agency. Congress should also explore whether Secretary Tillerson is in violation of the impoundment act, which prohibits any administration from unilaterally implementing proposed budget cuts without approval from Congress.[136]

Bolster defense assets in Europe

The Department of Defense should ensure that Europe remains a priority for critical defense assets that can ensure that the United States and NATO can deter Russian aggression. The Pentagon should continue to take steps to ensure that U.S. forces remain at the tip of the spear in NATO deployments by ensuring robust U.S. force deployments to NATO's east and south. The presence of U.S. forces could complicate Russian efforts to instigate a crisis. The Pentagon should also continue to prioritize the deployment to the European theater assets with high-deterrent value, such as F-22 fighters, and bolster maritime assets in the Baltic and Black seas.

Establish an Eastern European Security Assistance Initiative

Congress should establish an Eastern European Security Assistance Initiative through the State Department to help these countries transition from Russian military equipment without sacrificing short-term military readiness. Congress should help Eastern European states end their reliance on Russian equipment by providing a mix of financing and direct assistance to facilitate expensive fighter and helicopter acquisitions, just as the Bush administration did to help Poland procure F-16s in 2002.[139] Currently, countries, such as Bulgaria, are balancing expensive fighter acquisitions with maintaining short-term readiness. Congress should help these allies bolster their forces.

Maintain areas where there is useful cooperation with Russia and maintain a dialogue to avoid an escalatory trap

While Russia must be confronted, there are also areas where cooperation is both possible and in U.S. national interests. Russia, for instance, continues to implement the New START Treaty, which reduces Russian and U.S. nuclear arsenals and delivery vehicles. This treaty is in U.S. national security interests, so while Russia may violate other agreements, where it is in compliance and where it is in U.S. interests to continue, the United States should do so. Additionally, the United States and Russia should continue to maintain regular diplomatic contact. Russia shrinking the size of the U.S. diplomatic presence as retaliation against U.S. sanctions was done more out of weakness than strength, as Russia has few ways to overtly respond to the United States.

Fight the information war by significantly expanding public diplomacy efforts

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.[140] Meanwhile, many Western news networks decided it was not profitable enough to invest in foreign language media in small markets 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.[141] 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. 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. Congress should also ensure the Global Engagement Center (GEC) is resourced and empowered to counter Russian disinformation. While congress has authorized a significant increase in the GEC budget and expanded its mandate,[142] Secretary Tillerson has resisted these efforts.

Deter state-sponsored cyberattacks by sending clear message about U.S. cyber redlines

The United States needs to establish boundaries and deterrence in cyberspace through the clear messaging of U.S. cyber redlines and by loudly calling out cyberintrusions. 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 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.[143] 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.

Conclusion

Russia's attacks on American democracy and its efforts to undermine the United States and its allies have not stopped. Russia's actions are those of an adversary—not an ally or partner. It is delusional and harmful to the security of the United States for the Trump administration to continue to appease the Kremlin. The United States should not contemplate a new partnership or alliance with Russia without a clear and significant change in Russian behavior. While the Kremlin has shifted back to a Cold War-footing, the United States under President Trump has no coherent or unified approach. Congress has also done little and must take action now to improve America's defenses and protect U.S. democracy. Russia did not end its efforts to undermine American democracy with the 2016 election. The United States must prepare itself for the future attacks that are inevitably coming in the 2018 election.

About the authors

Max Bergmann is a senior fellow at American Progress, where he focuses on European security and U.S.-Russia policy. From 2011 to 2017, he served in the U.S. Department of State in a number of different positions, including as a member of the secretary of state's policy planning staff, where he focused on political-military affairs and nonproliferation; special assistant to the undersecretary for arms control and international security; speechwriter to then-Secretary of State John Kerry; and senior adviser to the assistant secretary of state for political-military affairs. Prior to serving in the State Department, he worked at American Progress as a military and nonproliferation policy analyst and at the National Security Network as the deputy policy director. Bergmann received his master's degree from the London School of Economics in comparative politics and his bachelor's degree from Bates College.

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

Endnotes

1 Max Bergmann and Carolyn Kenney, "War By Other Means: Russian Active Measures and the Weaponization of Information" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/.

2 BBC, "Trump Russia: US 'In Peril Over President's Stance,'" November 12, 2017, available at http://www.bbc.com/news/world-us-canada-41962023.

3 Ali Vitali, "Trump Backs Intel Agencies After Raising Doubts Over Russian Meddling," NBC News, November 12, 2017, available at https://www.nbcnews.com/politics/white-house/trump-clarifies-comments-putin-says-i-m-u-s-intel-n819986.

4 Sonam Sheth, "'This Implicates Us in Their Propaganda': The US Just Made a Striking Concession to the Kremlin," Business Insider, July 9, 2017, available at http://www.businessinsider.com/trump-putin-meeting-experts-cybersecurity-election-hacking-2017-7.

5 Hal Brands and Colin Kahl, "The Strategic Suicide of Aligning with Russia in Syria," *Foreign Policy*, February 7, 2017, available at http://foreignpolicy.com/2017/02/07/the-strategic-suicide-of-aligning-with-russia-in-syria/.

6 Laura Daniels, "How Russia Hacked the French Election," *Politico*, April 23, 2017, available at https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

7 Robbie Gramer and Dan De Luce, "State Department Scraps Sanctions Office," *Foreign Policy*, October 26, 2017, available at http://foreignpolicy.com/2017/10/26/state-department-scraps-sanctions-office/.

8 Esme Cribb, "Comey: Russia 'Will Be Back' to Interfere in Future US Elections," Talking Points Memo, June 8, 2017, available at http://talkingpointsmemo.com/livewire/comey-russia-will-be-back.

9 Ali Watkins, "Russia Escalates Spy Games after Years of U.S. Neglect," *Politico*, June 1, 2017, available at https://www.politico.com/story/2017/06/01/russia-spies-espionage-trump-239003.

10 Department of Homeland Security and Federal Bureau of Investigation, *Grizzly Steppe – Russian Malicious Cyber Activity* (2016), available at https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

11 U.S. Senate Select Committee on Intelligence, "Hearing of the Senate Select Committee for Intelligence," June 21, 2017, available at https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections.

12 Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatensfuture-u-s-elections.

13 Ibid.

14 Matthew Cole and others, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," The Intercept, June 5, 2017, available at https://theintercept.com/2017/06/05/top-secret-nsa-report-detail-srussian-hacking-effort-days-before-2016-election.

15 Ibid.

16 Ibid.

17 Timothy B. Lee, "Russia's Attempt to Hack US Election Officials, Explained," Vox, June 6, 2017, available at https://www.vox.com/new-money/2017/6/6/15745888/russia-election-hacking-leak.

18 Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatensfuture-u-s-elections.

19 Matthew Cole and others, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," The Intercept, June 5, 2017, available at https://theintercept.com/2017/06/05/top-secret-nsa-report-detail-srussian-hacking-effort-days-before-2016-election.

20 Lee, "Russia's Attempt to Hack US Election Officials, Explained."

21 U.S. Senate Select Committee on Intelligence, "Open Hearing on Russian Interference in the 2016 U.S. Elections," June 21, 2017, available at https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections.

22 Sam Jones and Ma 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.

23 Lily Hay Newman, "Russian Spies Helped Hack Yahoo, As If Tensions Weren't High Enough," *Wired,* March 15, 2017, available at https://www.wired.com/2017/03/yahoo-hack-russia-indictment/.

24 Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017, available at https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

25 Garrett M. Graff, "Inside the Hunt for Russia's Most Notorious Hacker," *Wired,* March 21, 2017, available at https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

26 Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017, available at https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

27 U.S. Department of Justice, "U.S. Charges Russian FSB Officers and their Criminal Conspirators for Hacking Yahoo and Millions of Emails," March 15, 2017, available at https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

28 Betsy Woodruff, "Feds: Russian Spies Paid Hackers to Break Into Yahoo," The Daily Beast, March 15, 2017, available at https://www.thedailybeast.com/feds-russian-spies-paid-hackers-to-break-into-yahoo.

29 Reuters, "Factbox: U.S. Arrests of Russian Cyber Criminals Hit Record High," August 25, 2017, available at https://www.reuters.com/article/us-russia-cyber-arrests-factbox/factbox-u-s-arrests-of-russian-cyber-criminals-hit-record-high-idUSKCN1B50M5.

30 The Associated Press, "A Look at Alleged Russian Cybercriminals Arrested in Europe," July 28, 2017, available at https://apnews.com/66955e6b62b44017a6e56cc99ead57f2.

31 Ibid.

32 Ibid.; Karolina Tagaris, "Greek Court Clears U.S. Extradition of Russian Bitcoin Fraud Suspect," Reuters, October 4, 2017, available at https://www.reuters.com/article/us-greece-russia-cyber-extradition/greek-court-clears-u-s-extradition-of-russian-bitcoin-fraud-suspect-idUSKCN1C90QR.

33 The Associated Press, "A Look at Alleged Russian Cybercriminals Arrested in Europe."

34 Ibid.

35 Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, available at https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

36 Matthew Rosenberg and Ron Nixon, "Kaspersky Lab Antivirus Software Is Ordered Off U.S. Government Computers," *The New York Times*, September 13, 2017, available at https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html.

37 Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *The New York Times*, October 10, 2017, available at https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

38 Sam Thielman, "Same Russian Hackers Likely Breached Olympic Drug-Testing Agency and DNC," *The Guardian*, August 22, 2016, available at https://www.theguardian.com/technology/2016/aug/22/russian-hackers-world-anti-doping-agency-dnc-hack-fancy-bear.

39 Ibid.

40 Euan McKirdy and Samantha Beech, "Olympic Ban Possible as Doping Body Labels Russia as Still 'Non-Compliant,'" CNN, available at http://edition.cnn.com/2017/11/16/sport/russia-doping-pyongchang-winter-olympics/index.html.

41 Watkins, "Russia Escalates Spy Games after Years of U.S. Neglect."

42 Scott Shane, Nicole Perlroth, and David Sanger, "Security Breech and Spilled Secrets Have Shaken the N.S.A. to Its Core," *New York Times,* November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html?_r=0.

43 Ibid.

44 Lily Hay Newman, "Wikileaks Just Dropped a Mega-Trove of CIA Hacking Secrets," *Wired,* March 7, 2017, available at https://www.wired.com/2017/03/wikileaks-cia-hacks-dump/.

45 Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, available at https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

46 Shane, Perlroth, Sanger, "Security Breech and Spilled Secrets Have Shaken the N.S.A. to Its Core."

47 Thomas Grove, Julian E. Barnes, and Drew Hinshaw, "Russia Targets NATO Soldier Smartphones, Western Officials Say," *The Wall Street Journal*, October 4, 2017, available at https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402.

48 Ben Schreckinger, "How Russia Targets the U.S. Military," *Politico*, June 12, 2017, available at https://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247.

49 Ellen Nakashima, "New Details Emerge About 2014 Russian Hack of the State Department: It Was 'Hand to Hand Combat,'" *The Washington Post*, April 3, 2017, available at https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html?utm_term=.b8251f0be627.

50 Bergmann and Kenney, "War By Other Means: Russian Active Measures and the Weaponization of Information."

51 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).

52 Andrew Weisburd, Clint Watts, and JM Berger, "Trolling for Trump: How Russia is Trying to Destroy Our Democracy," War on the Rocks, November 8, 2016, available at https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

53 Lindsay Smith and Ben Read, "APT28 Targets Hospitality Sector, Presents Threat to Travelers," FireEye, August 11, 2017, available at https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html.

54 Andy Greenberg, "Russia's 'Fancy Bear' Hackers Used Leaked NSA Tool to Target Hotel Guests," *Wired*, August 11, 2017, available at https://www.wired.com/story/fancy-bear-hotel-hack/.

55 Amie Ferris-Rotman, "The Diplomacy of Dog Walking," *Foreign Policy*, July 24, 2017, available at http://foreignpolicy.com/2017/07/24/the-diplomacy-of-dog-walking-in-russia-us-diplomat/.

56 Watkins, "Russia Escalates Spy Games After Years of U.S. Neglect."

57 Josh Rogin, "Russia Is Harassing U.S. Diplomats All Over Europe," *The Washington Post*, June 27, 2016, available at https://www.washingtonpost.com/opinions/global-opinions/russia-is-harassing-us-diplomats-all-over-europe/2016/06/26/968d1a5a-3bdf-11e6-84e8-1580c7db5275_story.html?utm_term=.b65a625ec47a.

58 Watkins, "Russia Escalates Spy Games After Years of U.S. Neglect."

59 Marshall Cohen and Jose Pagliery, "Nine months, nine prominent Russians dead," CNN, August 24, 2017, available at http://www.cnn.com/2017/03/24/europe/dead-russians/index.html.

60 NPR, "Clint Watts explains what he means by 'follow the trail of dead Russians,'" May 12, 2017, available at https://www.npr.org/2017/05/12/528072930/clint-watts-explains-what-he-means-by-follow-the-trail-of-dead-russians.

61 Heidi Blake and others, "From Russia with Blood, A BuzzFeed News Investigation," BuzzFeed, June 15, 2017, available at https://www.buzzfeed.com/heidiblake/from-russia-with-blood-14-suspected-hits-on-british-soil?utm_term=.shq2rZ5GZ#.ivaa3ZwAZ.

62 Jason Leopold and others, "From Russia with Blood, A BuzzFeed News Investigation," BuzzFeed, July 28, 2017, available at https://www.buzzfeed.com/jasonleopold/putins-media-czar-was-murdered-just-before-meeting-feds?utm_term=.bkPJ4eVWe#.xkzOPQERQ.

63 Mark Galeotti, "The Kremlin's Newest Hybrid Warfare Asset: Gangsters," *Foreign Policy*, June 12, 2017, available at http://foreignpolicy.com/2017/06/12/how-the-world-of-spies-became-a-gangsters-paradise-russia-cyberattack-hack/.

64 Mark Galeotti, "Crimintern: How the Kremlin uses Russia's Criminal Networks in Europe" (London: European Council on Foreign Relations, 2017), available at http://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

65 Brian Whitmore, "Putin's Mafia Statecraft," Radio Free Europe/Radio Liberty, October 27, 2015, available at https://www.rferl.org/a/putins-mafia-state-craft/27329898.html.

66 Brian Ross and Matthew Mosk, "Russian Mafia Boss Still At Large After After FBI Wiretap at Trump Tower," ABC News, March 21, 2017, available at http://abcnews.go.com/US/story-fbi-wiretap-russians-trump-tower/story?id=46266198.

67 Ibid.

68 Sebastian Rotella, "A Gangster Place in the Sun: How Spain's Fight Against the Mob Revealed Russian Power Networks," ProPublica, November 10, 2017, available at https://www.propublica.org/article/fighting-russian-mafia-networks-in-spain.

69 Mark Galeotti, "Crimintern."

70 Ciaran Martin, "Cyber Security: Fixing the Present, So we Can Worry About the Future," National Cyber Security Centre, November 15, 2017, available at https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future.

71 Jim Finkle, "U.S. Warns Businesses of Hacking Campaign Against Nuclear, Energy Firms," Reuters, June 30, 2017, available at https://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-businesses-of-hacking-campaign-against-nuclear-energy-firms-idUSKBN19L2Z9.

72 Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *The New York Times*, July 6, 2017, available at https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

73 Ellen Nakashima, "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks," *The Washington Post*, July 8, 2017, available at https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.dbd7b945a6c9.

74 Ibid.

75 Ellen Nakashima, "This Russian Cyber Weapon Could Wreak Havoc on U.S. Power Grids, New Research Says," *Chicago Tribune*, June 12, 2017, available at http://www.chicagotribune.com/bluesky/technology/ct-bsi-russia-cyber-weapon-that-can-disrupt-power-grids-20170612-story.html.

76 Andy Greenberg, "Hack Brief: Hackers Targeted a US Nuclear Plant (But Don't Panic Yet)," *Wired*, July 6, 2017, available at https://www.wired.com/story/hack-brief-us-nuclear-power-breach/.

77 Nakashima, "This Russian Cyber Weapon Could Wreak Havoc on U.S. Power Grids, New Research Says."

78 Michael Riley and Jordan Robertson, "FBI said to Examine Whether Russia Tied to JPMorgan Hacking," Bloomberg, August 27, 2014, available at https://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.

79 Stave Goldstein, "Alleged Russian spies in the U.S. were interested in high frequency trading," MarketWatch, May 26, 2016, available at https://www.marketwatch.com/story/russian-sentenced-over-spy-plan-that-included-high-frequency-trading-plot-2016-05-25.

80 Cameron Colquhoun, "Russia's next fake news campaign could devastate the economy," *Wired,* July 18, 2017, available at http://www.wired.co.uk/article/ghosts-in-the-machine.

81 Ibid.

82 Watkins, "Russia Escalates Spy Games After Years of U.S. Neglect."

83 David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times,* October 24, 2015, available at https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=2.

84 Vera Bergengruen, "Space war is coming – and Congress wants to create a U.S. 'Space Corps' to fight it," McClatchy, July 10, 2017 available at http://www.mcclatchydc.com/news/nation-world/national/article160609004.html.

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

86 Nafeesa Sayeed, "Pro-Russian Bots Sharpen Online Voting Attacks for 2018 U.S. Vote," Bloomberg, September 1, 2017, available at https://www.bloomberg.com/news/articles/2017-09-01/russia-linked-bots-hone-online-attack-plans-for-2018-u-s-vote.

87 Ibid.

88 Issie Lapowsky, "Facebook May Have More Russian Troll Farms to Worry About," *Wired*, September 8, 2017, available at https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/.

89 Casey Michel, "Russia-Linked Propaganda Accounts Banned by Twitter Are Still Active on Facebook," Think Progress, November 4, 2017, available at https://thinkprogress.org/russia-linked-propaganda-facebook-1ca727253ccf/.

90 Andrew Weisburd and Bret Schafer, "Insinuation and Influence: How the Kremlin Targets Americans Online," George Marshall Fund, October 16, 2017, available at http://securingdemocracy.gmfus.org/blog/2017/10/16/insinuation-and-influence-how-kremlin-targets-americans-online.

91 Gregory S. Schneider and Jenna Portnoy, "Did 'Bots' Inflame Online Anger Over Controversial Ad in VA Governor's Race," *The Washington Post*, November 4, 2017, available at https://www.washingtonpost.com/local/virginia-politics/did-bots-inflame-online-anger-over-controversial-ad-in-va-governors-race/2017/11/04/e2127c30-c186-11e7-959c-fe2b598d8c00_story.html?utm_term=.f67b2c682290.

92 Sayeed, "Pro-Russian Bots Sharpen Online Voting Attacks for 2018 U.S. Vote."

93 Christian Caryl, "Here are Some of the Craziest Fake Stories that Russia Launched in the Past Three Weeks," *The Washington Post,* November 15, 2017, available at https://www.washingtonpost.com/news/democracy-post/wp/2017/11/15/here-are-some-of-the-craziest-fake-stories-that-russia-launched-in-the-past-three-weeks/?utm_term=.81b1bee68fbd.

94 Ibid.

95 Andrew Weisburd and Bret Schafer, "Insinuation and Influence: How the Kremlin Targets Americans Online," German Marshall Fund's Alliance for Securing Democracy, October 16, 2017, available at http://securingdemocracy.gmfus.org/blog/2017/10/16/insinuation-and-influence-how-kremlin-targets-americans-online.

96 Radio Free Europe/Radio Liberty, "Putin Says U.S. Pressure on RT an 'Attack,' Will Get 'Proper Response,'" November 11, 2017, available at https://www.rferl.org/a/russia-today-rt-justice-department-deadline-register-foreign-agent/28844886.html.

97 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.

98 BBC, "Russia 'Was Behind German Parliament Hack,'" May 13, 2016, available at http://www.bbc.com/news/technology-36284447.

99 Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?" *BBC*, April 3, 2017, available at http://www.bbc.com/news/world-europe-39478066.

100 Juliet Perry, "Putin Meets French Far-Right Candidate Marine Le Pen at Kremlin," CNN, March 24, 2017, available at http://www.cnn.com/2017/03/24/europe/putin-le-pen-kremlin/index.html.

101 Cynthia Kroet, "Russia Spread Fake News During Dutch Election: Report," *Politico*, April 4, 2017, available at https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/.

102 Anabel Diez, "Government Confirms Intervention of Russian Hackers in Catalan Crisis," *El Pais*, November 10, 2017, available at https://elpais.com/elpais/2017/11/10/inenglish/1510329788_994258.amp.html.

103 Casey Michel, "Why Russia Loves the Idea of California Seceding," *Politico*, January 15, 2017, available at https://www.politico.com/magazine/story/2017/01/why-russia-loves-the-idea-of-california-seceding-214632.

104 Casey Michel, "Putin's Plot to Get Texas to Secede," *Politico*, June 22, 2015, available at https://www.politico.com/magazine/story/2015/06/vladimir-putin-texas-secession-119288.

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

106 Steven Pifer, "Mr. Lavrov, Russia, and the Budapest Memorandum," Brookings Institution, January 28, 2016, available at https://www.brookings.edu/blog/order-from-chaos/2016/01/28/mr-lavrov-russia-and-the-budapest-memorandum/.

107 Tim Hume and Claudia Rebaza, "MH17 Shot Down by Buk Missile Brought from Russia, Say Investigators," CNN, September 28, 2016, available at http://www.cnn.com/2016/09/28/europe/mh17-buk-russia/index.html.

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

109 Andrew Kramer, "Bomb Wounds Ukrainian Politician as Assassination Plots Mount," *The New York Times*, October 25, 2017, available at https://www.nytimes.com/2017/10/25/world/europe/ukraine-kiev-bomb-assassination.html.

110 BBC, "UN Accuses Russia of Violating Human Rights in Crimea," September 25, 2017, available at http://www.bbc.com/news/world-europe-41386490.

111 Gregory Hellman and Bryan Bender, "The Other Treaty on the Chopping Block," *Politico*, June 24, 2017, available at https://www.politico.com/story/2017/06/24/nuclear-arms-treaty-russia-trump-239923 ; Michael R. Gordon, "Russia Has Deployed Missile Barred by Treaty, U.S. General Tells Congress," *The New York Times*, March 8, 2017, available at https://www.nytimes.com/2017/03/08/us/politics/russia-inf-missile-treaty.html.

112 Jim Garamone, "EUCOM Chief Makes Case for Continued Funding for the European Reassurance Initiative," DoD News, May 3, 2017, available at https://www.defense.gov/News/Article/Article/1171280/eucom-chief-makes-case-for-continued-funding-for-european-reassurance-initiative/.

113 Kathleen Joyce, "Russian Jet Buzzes US Recon Jet: Pictures Released of 'Unsafe Incident,'" Fox News, June 23, 2017, available at http://www.foxnews.com/us/2017/06/23/russian-jet-buzzes-us-recon-jet-pictures-released-unsafe-incident.html.

114 Raf Sanchez, "Russian Jet Flies 'Within Five Feet' of US Aircraft Over the Baltic," The Telegraph, June 21, 2017, available at http://www.telegraph.co.uk/news/2017/06/21/russian-jet-flies-within-five-feet-us-aircraft-baltic/.

115 Teri Schultz, "NATO Says More Russian Buzzing of Baltic Airspace a Risk for Deadly Mistakes," *DW*, June 27, 2017, available at http://www.dw.com/en/nato-says-more-russian-buzzing-of-baltic-airspace-a-risk-for-deadly-mistakes/a-39440788.

116 Zachary Cohen and Pamela Boykoff, "NATO Jet Intercepts Russian Minister's Plane," CNN, June 23, 2017, available at http://www.cnn.com/2017/06/21/politics/nato-jet-russian-defense-minister-aircraft/index.html.

117 Schultz, "NATO Says More Russian Buzzing of Baltic Airspace a Risk for Deadly Mistakes."

118 Reuters, "Russia Moves Nuclear-Capable Missiles into Kaliningrad," October 8, 2016, available at https://www.reuters.com/article/us-russia-usa-missiles-confirm/russia-moves-nuclear-capable-missiles-into-kaliningrad-idUSKCN1280IV.

119 Sergey Sukhankin, "Kaliningrad: From Boomtown to Battle-Station," European Council on Foreign Relations, March 27, 2017, available at http://www.ecfr.eu/article/commentary_kaliningrad_from_boomtown_to_battle_station_7256#.

120 Mathieu Boulegue, "Five Things to Know About the Zapad Exercise," Chatham House, September 25, 2017, available at https://www.chathamhouse.org/expert/comment/five-things-know-about-zapad-2017-military-exercise.

121 John Irish, Stephanie Nebehay, and Tom Miles, "One Question at U.N. Syria Talks: What Does Russia Want?", Reuters, February 24, 2017, available at https://www.reuters.com/article/us-mideast-crisis-syria-un-russia/one-question-at-u-n-syria-talks-what-does-russia-want-idUSKBN16324L.

122 BBC, "Migrant Crisis: Russia and Syria 'Weaponising' Migration," March 2, 2016, available at http://www.bbc.com/news/world-europe-35706238.

123 Brands and Kahl, "The Strategic Suicide of Aligning with Russia in Syria."

Gramer and De Luce, "State Department Scraps Sanctions Office."

124 Joby Warrick, "How Russia Quietly Undermines Sanctions Intended to Stop North Korea's Nuclear Program," *The Washington Post*, September 11, 2017, available at https://www.washingtonpost.com/world/national-security/how-russia-quietly-undercuts-sanctions-intended-to-stop-north-koreas-nuclear-program/2017/09/11/f963867e-93e4-11e7-8754-d478688d23b4_story.html?utm_term=.9e16bbc052d4.

125 Zeeshan Aleem, "Why Russia and China Watered Down the UN's New North Korea Sanctions," Vox, September 12, 2017, available at https://www.vox.com/world/2017/9/12/16294020/russia-china-water-un-sanction-north-korea.

126 Jennifer Rankin, "Russian Destabilisation of Balkans Rings Alarm Bells as EU Leaders Meet," *The Guardian*, March 9, 2017, available at https://www.theguardian.com/world/2017/mar/08/top-mep-says-eu-must-do-more-to-stop-russia-destabilising-balkans.

127 Mariana Parraga and Alexandra Ulmer, "Russia's Biggest Oil Company Has Been Secretly Helping Maduro Stay Afloat in Venezuela," *Business Insider*, August 11, 2017, available at http://www.businessinsider.com/r-special-report-vladimirs-venezuela-leveraging-loans-to-caracas-moscow-snaps-up-oil-assets-2017-8.

128 U.S. Department of State, "Remarks by Secretary of State Rex Tillerson," August 22, 2017, available at https://www.state.gov/secretary/remarks/2017/08/273577.htm.

129 Idrees Ali, "Top U.S. General in Afghanistan Sees Russia Sending Weapons to Taliban," Reuters, April 24, 2017, available at https://www.reuters.com/article/us-usa-afghanistan-russia/top-u-s-general-in-afghanistan-sees-russia-sending-weapons-to-taliban-idUSKBN17Q1H2.

130 Michael Sozan, "On HAVA's 15th Anniversary, Congress Needs to Make U.S. Elections More Secure" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/10/26/441417/on-havas-15th-anniversary-congress-needs-to-make-u-s-elections-more-secure/.

131 Ibid.

132 Reuters, "Saudi Arabia Agrees to Buy Russian S-400 Air Defense System: Arabiya TV," Reuters, October 5, 2017, available at https://www.reuters.com/article/us-saudi-russia-missiles/saudi-arabia-agrees-to-buy-russian-s-400-air-defense-system-arabiya-tv-idUSKBN1CA1OD.

133 Vivian Salama and Julie Pace, "Trump Has Embraced Autocratic Leaders Without Hesitation," *Chicago Tribune*, April 19, 2017, available at http://www.chicagotribune.com/news/nationworld/politics/ct-trump-erdogan-xi-20170419-story.html.

134 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.

135 Karen Hobart Flynn, "Congress It Is Time for You To Do What Tech Giants Refuse To Do," The Daily Beast, November 13, 2017, available at https://www.thedailybeast.com/congress-its-time-for-you-to-do-what-the-tech-giants-refuse-to-6.

136 U.S. Department of the Treasury, "Advisory to Financial Institutions and Real Estate Firms and Professionals," Financial Crimes Enforcement Network (FinCen) Advisory, August 22, 2017, available at https://www.fincen.gov/sites/default/files/advisory/2017-08-22/Risk%20in%20Real%20Estate%20Advisory_FINAL%20508%20Tuesday%20%28002%29.pdf.

137 Max Bergmann, "Present at the Destruction: How Rex Tillerson Is Wrecking the State Department," *Politico,* available at https://www.politico.com/magazine/story/2017/06/29/how-rex-tillerson-destroying-state-department-215319.

138 Daniel Benaim, "Here's How Congress Can Save the State Department," *Foreign Policy*, September 11 2017, available at http://foreignpolicy.com/2017/09/11/heres-how-congress-can-save-the-state-department/.

139 Aerospace Daily & Defense Report, "Congress approves $3.8B loan to Poland for F-16 purchase," October 14, 2002, available at http://aviationweek.com/awin/congress-approves-38b-loan-poland-f-16-purchase.

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

141 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.

142 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.

143 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.

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