THE NEW GEOPOLITICS
EUROPE

MARCH 2018

THE FUTURE OF POLITICAL WARFARE: RUSSIA, THE WEST, AND THE COMING AGE OF GLOBAL DIGITAL COMPETITION

ALINA POLYAKOVA
SPENCER P. BOYER

BROOKINGS – ROBERT BOSCH FOUNDATION
TRANSATLANTIC INITIATIVE

THE FUTURE OF POLITICAL WARFARE: RUSSIA, THE WEST, AND THE COMING AGE OF GLOBAL DIGITAL COMPETITION

ALINA POLYAKOVA
SPENCER P. BOYER

EXECUTIVE SUMMARY

The Kremlin's political warfare against democratic countries has evolved from overt to covert influence activities. But while Russia has pioneered the toolkit of asymmetric measures for the 21st century, including cyberattacks and disinformation campaigns, these tools are already yesterday's game. Technological advances in artificial intelligence (AI), automation, and machine learning, combined with the growing availability of big data, have set the stage for a new era of sophisticated, inexpensive, and highly impactful political warfare. In the very near term, it will become more difficult, if not impossible, to distinguish between real and falsified audio, video, or online personalities. Malicious actors will use these technologies to target Western societies more rapidly and efficiently. As authoritarian states such as Russia and China invest resources in new technologies, the global competition for the next great leap in political warfare will intensify. As the battle for the future shifts to the digital domain, policymakers will face increasingly complex threats against democracies. The window to mount an effective "whole-of-society" response to emerging asymmetric threats is quickly narrowing.

This paper outlines the current state of play in political warfare, identifies emerging threats, and proposes potential policy responses. It argues for greater information sharing mechanisms between trans-Atlantic governments and the private sector, greater information security and transparency, and greater investments in research and development on AI and computational propaganda. As authoritarian regimes seek to undermine democratic institutions, Western societies must harness their current—though fleeting—competitive advantage in technology to prepare for the next great leap forward in political warfare. Western governments should also develop a deterrence strategy against political warfare with clearly defined consequences for specific offensive actions, while ensuring they retain their democracies' core values of openness and freedom of expression.

INTRODUCTION: THE EVOLUTION OF RUSSIAN POLITICAL WARFARE FROM UKRAINE TO THE UNITED STATES

In November 2004, Ukraine's presidential election was contested by two candidates: a pro-Western independent, Viktor Yushchenko, versus the Russian-backed prime minister, Viktor Yanukovych. In the run up to election day, Yushchenko was mysteriously poisoned and left permanently disfigured. On voting day, districts loyal to the pro-Russian candidate suddenly acquired millions of new voters; masked men showed up to some polling stations to harass opposition supporters; and many Ukrainians "rose from the dead" to cast their votes for Yanukovych, who was declared the winner. These crude and obvious tactics to swing the election resulted in mass protests that led to a second round of voting, which then swept Yushchenko to the presidency.

Ten years later, in 2014, Ukraine, having just undergone another revolution and now in open conflict with Russia in the Donbas, was once again holding important presidential elections, and once again, there was an attempt to swing the vote. But this time, the tactics were starkly more sophisticated: instead of poisoning, masked thugs, and ballot stuffers, Russia-linked cyber hackers infiltrated Ukraine's central election commission, deleting key files and implanting a virus that would have changed the results of the election in favor of a fringe ultra-nationalist party, Right Sector. Government cybersecurity experts detected the vote-altering malware less than an hour before the election results were announced. In a surreal twist, however, the Russian state media still reported the fake results, showing the ultra-nationalists winning, though in reality, Right Sector received less than 1 percent of the vote.[1] At the time, cybersecurity experts called the Ukraine hack one of the most brazen, malicious, and grand-scale attempts to manipulate a national election ever. The United States and Europe should have been paying attention because some of the same tools deployed in Ukraine would resurface in the U.S. presidential election two years later.

During the decade between Ukraine's two presidential elections, the Kremlin's "active measures"—covert activities aimed at influencing politics, narratives, and policies in favor of Russia's geopolitical interests—evolved from overt to covert, physical to digital, conventional to asymmetric. The new tools are cheaper, faster, and allow for maximum plausible deniability. But they are also less precise, and thus ripe with potential unintended consequences and ambiguous results. Ukraine and other post-Soviet states have been a testing ground for Russia's 21st century arsenal of active measures.

By 2016, when Moscow turned its attention to the U.S. presidential election, the tactics, while familiar, were also savvier. Russia and its proxies combined cyberattacks with psychological operations and exploited social media platforms to stoke societal tensions and discredit the anti-Kremlin candidate, Hillary Clinton. In January 2017, the U.S. intelligence community concluded in an unclassified report that in the U.S. presidential election, "Russia's goals were to undermine public faith in the U.S. democratic process" through a "strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian government agencies" and proxies.[2] Indeed, in

[1] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

[2] "Background to 'Assessing Russian activities and intentions in recent U.S. elections': The analytic process and cyber incident attribution," U.S. Office of the Director of National Intelligence, January 7, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

the elections that followed in Europe, Russia's fingerprints were visible everywhere to varying degrees: from the attempts by Russia-linked trolls (human-curated fake accounts) and bots (automated accounts) to spread "fake news" about the French presidential candidate Emmanuel Macron in the spring of 2017 to a disinformation campaign around the Catalan independence referendum in Spain that October. In each case, the tools and objectives were the same: the use of disinformation campaigns, cyberattacks, cultivation of political allies and proxies, and political subversion in order to divide, destabilize, and deceive democratic societies.

Russian influence operations do not focus on isolated events. Rather, taken as whole, they are at the core of a political strategy—honed in Europe's East and deployed against the West—to weaken Western institutions and undermine trans-Atlantic consensus. As such, Moscow's efforts of political warfare work in mutually reinforcing, though not always in clearly coordinated, ways, akin to an evolving ecosystem. This ecosystem consists of a web of proxy actors and cut-outs—media organizations, social media accounts, vested business interests, oligarchs, civil society groups, cyber criminals, intelligence agencies, private companies, and political actors inside and outside of Russia. Some of these players act at the direct behest of the Kremlin, and others out of their own political agenda, but with the same ultimate result. The ecosystem is a moving target: continuously evolving in its sophistication, multilayered in its complexity, and purposely hidden.

The political warfare threat extends beyond Russia. While the Kremlin has been a key actor in developing the toolkit, these tools are appealing to other malicious state and non-state actors seeking to undermine democracies. The evolution of technology—and Russia's and China's stated desire to lead on artificial intelligence (AI) research—signals that Western democracies will face increasing threats in the cyber and information domain.

> **The political warfare threat extends beyond Russia.** ”

Just as authoritarian regimes learn from each other, Western governments, civil society, and the private sector will need to establish avenues for sharing best practices of resistance and deterrence. Furthermore, if Western democracies hope to avoid being taken by surprise again, public and private sector stakeholders will need to think beyond reacting to attacks on elections and more about identifying—and preparing for—the emerging threats that will advance asymmetrical capabilities in the very near term. As authoritarian regimes seek to undermine democratic institutions, Western societies must harness their current—though fleeting—competitive advantage in technology to prepare for the next great leap forward in political warfare, especially AI. The West can no longer afford to play yesterday's game. To better equip Western societies to deal with this emerging reality, this paper outlines the current state of the Kremlin's toolkit, near-term emerging threats, and potential policy responses.

CURRENT STATE OF PLAY: A PRIMER ON THE RUSSIAN TOOLKIT

State actors have been the main drivers of political warfare against the West. While non-state terrorist groups, such as ISIS, have been effective in using propaganda for recruitment purposes, they lack the resources to scale up their operations. Under Vladimir Putin, Russia has sought to expand its arsenal of "active measures"—tools of political warfare once used by the Soviet Union that aimed to influence world events through the manipulation of media, society, and politics—to deploy against democracies.[1]

The Kremlin's strategy of influence includes: disinformation campaigns, the cultivation of political allies in European democracies, and cyberattacks. In each instance, multiple layers of proxies, which are direct or indirect Kremlin agents and entities, are employed to maintain plausible deniability and strategic ambiguity. This Russian-developed toolkit represents the current state of play of political warfare. The following offers a rough sketch of how these parallel streams of interference operate.

Disinformation

Key actors

- **Overt:** Russian state media such as *RT*, *Sputnik*, *Ruptly TV*.
- **Covert:** Social media trolls (e.g., the Internet Research Agency, or IRA);[2] automated accounts (bots); impersonation accounts on Facebook, Twitter, and Instagram; WikiLeaks; DCLeaks.

Goals

- Undermine the Western political narrative and trans-Atlantic institutions.
- Sow discord and divisions within countries.
- Blur the line between fact and fiction.

Methods

- **Full-spectrum dissemination and amplification of misleading, false, and divisive content.** Overtly, Moscow has expanded its reach through channels in English, Spanish, German, Arabic, and French, which often piggyback on current events to insert false and misleading stories. To buttress the state-run media outlets, digital bot and troll armies amplify divisive and/or misleading content online.
- **Deployment of computational propaganda.** The spread of propaganda through technical, often automated, means to deliberately sway public opinion.[3] Russia-linked social media accounts on Twitter and Facebook are particularly adept at coupling automation (bots) with human curation to disseminate and spread counter-Western narratives.
- **Identification of societal vulnerabilities.** Russia-linked actors often amplify divisive social issues. In Europe, those issues tend to focus on national sovereignty and immigration, Islam, terrorism, and the EU as a globalist, elitist body. In the United States, Russia's disinformation machine has focused

[1] Alina Polyakova, Marlene Laruelle, Stefan Meister, and Neil Barnett, "The Kremlin's Trojan horses," (Washington, DC: Atlantic Council, November 2016), http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses.

[2] Thirteen Russian nationals associated with the IRA were indicted by the U.S. Department of Justice on February 15, 2018, as part of the special counsel investigation into foreign interference in the 2016 U.S. election. The indictment documents how the IRA, based in St. Petersburg, Russia, carried out an intelligence and influence operation against the United States that included disinformation, impersonation of U.S. citizens, and intelligence gathering in the United States. See United States of America v. Internet Research Agency LLC et al., Criminal no. (18 U.S.C. §§ 2, 371, 1349, 1028A), https://www.justice.gov/file/1035477/download.

[3] Gillian Bolsover and Philip Howard, "Computational propaganda and political big data: Moving toward a more critical research agenda," *Big Data 5*, no. 4 (2017): 273-76, http://online.liebertpub.com/doi/abs/10.1089/big.2017.29024.cpr?journalCode=big.

on racial tensions, criminal justice policy, immigration from Latin American and Muslim-majority countries, and class divisions.

Examples

- **The "Lisa" case (Germany, January 2016):** Perhaps the most widely reported Russian disinformation operation in Europe concerned a 13-year-old Russian-German girl named "Lisa."[4] Russia's *Channel One*—a Kremlin channel broadcasting into Germany in Russian—initially reported that Lisa, who had been missing for 30 hours, was sexually assaulted by migrants in Germany. German police quickly determined that the story was false, and Lisa herself admitted that she was with friends during the time. But it was too late: the story was amplified by German and English-language Russian media (*RT* and *Sputnik*), and was widely disseminated on social media, eventually leading to anti-immigrant and anti-Angela Merkel demonstrations. In the end, the story was traced back to a Facebook group and anti-refugee website called *Asylterror* with Russian links. But even after German police debunked the story, Russian Foreign Minister Sergey Lavrov continued to promote it and criticize Germany.[5]
- **Anti-NATO propaganda (Sweden, August 2016):** Sweden faced an onslaught of fake stories about the negative consequences of any moves to enter into a military partnership with NATO, including untruthful claims about the alliance plotting to stockpile nuclear weapons on Swedish soil, NATO's prerogative to attack Russia from Swedish territory without Stockholm's consent, and NATO soldiers having license to sexually assault Swedish women without fear of prosecution because of legal immunity.[6]
- **Presidential election (United States, 2016):** The multi-vector information war against the United States is the most detailed account of Russian political warfare against a Western democracy to date. As a 2017 U.S. intelligence report and the 2018 Department of Justice indictment[7] against Russian actors detailed, the Russian government funded a methodical effort to undermine the 2016 U.S. presidential election. Russian operatives associated with the IRA impersonated Americans online and created fake personas and groups on social media to pit different segments of U.S. society against each other. The IRA relied especially on Facebook and Instagram to create fake "activist groups" on divisive social issues, including the Black Lives Matter movement, religion, immigration, and others. It also created Twitter accounts that spread disparaging stories about Hillary Clinton, misinformation about voting, and divisive content. The IRA also purchased political ads and organized political rallies in battleground states. These covert efforts were amplified by *RT*, *Sputnik*, and other Russian media outlets and began as early as 2014.
- **#MacronLeaks (France, April-May 2017):** French President Emmanuel Macron was the target of Russia-linked disinformation operations in the spring of 2017. Russian intelligence agents created bogus Facebook personas in order to spy on then-candidate Macron.[8] Facebook later acknowledged that it had identified numerous fake accounts that were spreading disinformation about the French election.[9] In addition, a trove of emails were hacked from Macron campaign officials. Even though

[4] Stefan Meister, "The 'Lisa case': Germany as a target of Russian disinformation," *NATO Review*, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

[5] Jakub Janda and Ilyas Sharibzhanov, "Six outrageous lies Russian disinformation peddled about Europe in 2016," *Atlantic Council*, http://www.atlanticcouncil.org/blogs/ukrainealert/six-outrageous-lies-russian-disinformation-peddled-about-europe-in-2016.

[6] Neil MacFarquhar, "A powerful Russian weapon: The spread of false stories," *The New York Times*, August 28, 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

[7] United States of America v. Internet Research Agency LLC et al.

[8] Joseph Menn, "Exclusive: Russia used Facebook to try to spy on Macron campaign – sources," *Reuters*, July 27, 2017, https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI.

[9] Ibid.

EMERGING THREATS

The future of political warfare is in the digital domain. The influence tools used by Moscow against the West are still fairly basic: they rely on exploiting human gullibility, vulnerabilities in the social media ecosystem, and lack of awareness among publics, the media, and policymakers. In the three-to-five year term, however, these tools will become more advanced and difficult to detect. In particular, technological advancements in artificial intelligence and cyber capabilities will open opportunities for malicious actors to undermine democracies more covertly and effectively than what we have seen so far.[3] In addition, increasingly sophisticated cybertools, tested primarily by Russia in Eastern Europe, have already affected Western systems. An attack on Western critical infrastructure seems inevitable.

[3] Tim Hwang, "Digital disinformation: A primer," (Washington, DC: Atlantic Council, September 2017), http://www.atlanticcouncil.org/publications/articles/digital-disinformation-a-primer.

the emails were dumped publicly just two days before the elections, during the period when media were no longer allowed to report on the elections in accordance with French law, the Twitter campaign #MacronLeaks reached 47,000 tweets in just 3.5 hours after the initial tweet.[10]

Political networks

Key actors

- **Aligned or friendly political parties:** Many, but not all, far-right and far-left political parties in Europe have adopted a pro-Kremlin stance to varying degrees. On one side of the spectrum are political parties that have signed explicit cooperation agreements with Putin's United Russia Party, including the French National Front (FN), the Austrian Freedom Party (FPÖ), the youth wing of Germany's Alternative for Germany (AfD), Germany's The Left (Die Linke), and the Italian League (Lega). Others have repeatedly advocated for pro-Russian policies, such as the removal of sanctions and recognition of Crimea as Russian territory. Leaders of the Italian 5 Star Movement (M5S), Spanish Podemos, Greece's Syriza and Golden Dawn, the British United Kingdom Independence Party (UKIP), the Hungarian Jobbik, and the Dutch Party for Freedom (PVV) have all made frequent pro-Putin and pro-Kremlin statements.[11]

Goals

- Undermine European politics from within by supporting insurgent anti-establishment, anti-EU political movements.
- Weaken European consensus on a common policy toward Russia by drawing divisions between European states and between the EU and the United States.

Methods

- Financial support, diplomatic support, and media and public relations support.

[10] "Hashtag campaign: #MacronLeaks," *DRFLab*, May 5, 2017, https://medium.com/dfrlab/hashtag-campaign-macronleaks-4a3fb870c4e8.

[11] Party platforms classified as pro-Russian based on Alina Polyakova et al., "The Kremlin's Trojan horses."

The evolution of AI and computational propaganda

In today's online environment, private companies are able to effectively detect bots, trolls, and other forms of manipulation. Computational propaganda—"the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"—can be tracked and monitored by tech savvy investigative researchers and groups.[4] Detection is still possible because these tactics still depend on human curation and, once the capabilities are acquired, are deployed in predictable patterns. But these tools are about to become far more complicated and difficult to counter.

[4] Samuel C. Woolley and Philip N. Howard, "Computational propaganda worldwide: Executive summary," *Oxford Internet Institute*, June 19, 2017, https://www.oii.ox.ac.uk/blog/computational-propaganda-worldwide-executive-summary/.

Examples

- **France—National Front campaign financing:** The FN is the only known example of Russian financial backing for a far-right party in Europe. In 2014, the party received a loan of approximately $9.8 million and in 2017, the party's leaders and then-presidential candidate, Marine Le Pen, requested an additional $29 million loan from Russia.[12] In addition to financial backing, Le Pen has sought to develop a personal relationship with Putin, having made several high-level visits to Russia while being his strongest advocate at home.
- **2017 German federal elections and the AfD:** The anti-immigrant AfD—now the third-largest party in the German parliament—is forging closer ties with Moscow and has repeatedly called for a more harmonious relationship with Moscow.[13] The AfD has established tighter connections between its youth wing and the youth organization of the Kremlin's United Russia party, and has done robust outreach to Russian-German voters.[14] Notably, in February 2017, the speaker of the Russian parliament (Duma), Vyacheslav Volodin, met with then-AfD Chairwoman Frauke Petry in Moscow to discuss interparty cooperation, while the AfD has fielded Russian-speaking Germans with anti-migrant views as candidates.[15] In addition, Russian state-controlled media provided favorable coverage to the AfD, its candidates, and messaging in the lead-up to the September 2017 German election.[16] The AfD's results in the September election were above average in areas with large Russian-speaking populations, such as Pforzheim in Baden-Württemberg.[17]

[12] James McAuley, "France's National Front faces funding shortfall before the 2017 election," *The Washington Post*, December 22, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/12/22/frances-national-front-faces-funding-shortfall-before-the-2017-election/?utm_term=.4c624da4ea3a.

[13] Ken Gude, "Russia's 5th column," *Center for American Progress*, March 15, 2017, https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/.

[14] Melanie Amann and Pavel Lokshin, "German populists forge deeper ties with Russia," *Spiegel Online*, April 27, 2016, http://www.spiegel.de/international/germany/german-populists-forge-deeper-ties-with-russia-a-1089562.html.

[15] Paul Stronski and Richard Solosky, "The return of global Russia: An analytical framework," (Washington, DC: Carnegie Endowment for International Peace, December 2017), http://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.

[16] Ibid.

[17] Maria Snegovaya, "Russian propaganda in Germany: More effective than you think," *The American Interest*, October 17, 2017, https://www.the-american-interest.com/2017/10/17/russian-propaganda-germany-effective-think/.

Online social media bots follow distinguishable patterns when they are "turned on" to spread disinformation: multiple accounts become active simultaneously and publish similar content on a schedule; the content is repetitive and nonsensical; and it is published at non-human speeds. These automated accounts are used primarily to amplify divisive content produced by human-curated accounts, state-controlled media (e.g., *RT*), or other proxies, and to attack specific individual or groups. Cyber intelligence analysis relies on those sets of metrics, among others, to attribute specific activities to known groups and identify bot networks.

While the social media environment is particularly vulnerable to manipulation through computational propaganda, the companies in this field are still ahead of the curve in their ability to identify coordinated automated campaigns (once they know what they are looking for). To do so, tech companies use AI tools and machine learning in their algorithms to detect coordinated bot networks, extremist content, and attempts to

- **Support for separatists:** Given Moscow's view that separatist movements serve as a powerful and visible wedge to divide and weaken the West, Russia has been an ally to European separatist groups on the left and the right. Most recently, the Catalan independence referendum in October 2017 received a chilly reception from the West, including the United States and the European Union, which backed Madrid's effort to delegitimize the vote. Russia (along with Venezuela and Scotland), however, backed the Catalan bid, with a propaganda campaign that deployed its state-owned media outlets and social media bots to support the separatists' narratives.[18] Moscow has worked to capitalize on these connections by convening both far-right parties and separatist movements to discuss best practices for furthering common agendas in a global movement.[19] Moscow hosted the International Russian Conservative Forum in March 2015 in St. Petersburg, convening ultranationalist political leaders from across Europe.[20] The Kremlin also brought together secessionist representatives from Scotland, Catalonia, the Basque country, northern Italy, Northern Ireland, and other locations at a conference in Moscow in 2017.[21]
- **Support for would-be authoritarians:** At the personal level, Moscow is adept at using democratically elected, influential individuals themselves to delegitimize systems from within.[22] Russia's brand of anti-Western authoritarianism is appealing and inspirational to European leaders who seek to style themselves in opposition to Western liberalism. Hungarian Prime Minister Viktor Orbán and Slovakian Prime Minister Robert Fico, for example, have publicly or privately identified Russia as a political model from which to learn and to emulate.[23]

[18] Editorial Board, "Catalonia held a referendum. Russia won," *The Washington Post*, October 2, 2017, https://www.washingtonpost.com/opinions/global-opinions/catalonia-held-a-referendum-russia-won/2017/10/02/f618cd7c-a798-11e7-92d1-58c702d2d975_story.html.

[19] "Russian influence in Europe: Six ways (other than hacking) that Russia is exploiting divisions and the rise of xenophobia in Europe," (New York: Human Rights First, January 11, 2017), https://www.humanrightsfirst.org/resource/russian-influence-europe.

[20] Gabrielle Tetrault, "Russian, European far-right parties converge in St. Petersburg," *The Moscow Times*, March 22, 2015, https://themoscowtimes.com/articles/russian-european-far-right-parties-converge-in-st-petersburg-45010.

[21] Casey Michel, "U.S. and EU separatist groups to gather on Moscow's dime," *The Diplomat*, July 26, 2016, https://thediplomat.com/2016/07/us-and-eu-separatist-groups-to-gather-on-moscows-dime/.

[22] Alina Polyakova et al., "The Kremlin's Trojan horses."

[23] Heather Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, "The Kremlin playbook." (Washington, DC: Center for Strategic and International Studies, October 2016), 6-7, https://www.csis.org/analysis/kremlin-playbook.

manipulate content rankings.[5] These tools are far more limited in their ability to detect divisive content around social issues being amplified by both real and fake users.

In the very near term, the evolution of AI and machine learning, combined with the increasing availability of big data, will begin to transform human communication and interaction in the digital space. It will become more difficult for humans and social media platforms themselves to detect automated and fake accounts, which will become increasingly sophisticated at mimicking human behavior. AI systems will be able to adapt to new contexts, suggest relevant original content, interact more sensibly with humans in proscribed contexts, and predict human emotional responses to that content. They will be able to access and analyze information that people share about themselves

[5] Machine learning is part of AI and refers to the ability of computers to analyze large amounts of data, recognize patterns, learn from them, and then predict or act without human programming. Machines are thus "trained" to complete tasks without human intervention. See Michael Copeland, "The difference between AI, machine learning, and deep learning?" *The Official NVIDIA Blog*, July 29, 2016, https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/.

Cyberattacks in the service of disinformation campaigns

Key actors

- **Government agencies:** Military Intelligence Service (GRU), Federal Security Service (FSB), Foreign Intelligence Service (SVR).
  - **Known proxies:** Advanced Persistent Threats (APT) 28 and 29,[24] CyberBerkut.
- **Supporting actors:** WikiLeaks, DCLeaks, Shadow Brokers.
- **Informal proxies:** cyber criminals, tech firms, cyber "activists."

Goals

- Discredit and delegitimize democratic elections.
- Sow distrust in Western institutions by revealing politically damaging information.

Methods

- Theft of personal and institutional information, which is later leaked online by a self-proclaimed independent group (e.g., WikiLeaks) and then used to spin a disinformation campaign to damage particular individuals (e.g., Hillary Clinton) or institutions (e.g., the U.S. National Security Agency, NSA).
- On a technical level, the methods are well known, relying primarily on user error and cybersecurity vulnerabilities.
  - **Spear phishing:** Targeted attempts to steal sensitive information, such as account credentials or financial information, through a tailored electronic attack. Most commonly, victims (individuals or organizations) will receive an email from a seemingly trusted source that will expose the user to malware or compel him or her to divulge account login information.
  - **Denial of service attacks:** Attempts to prevent legitimate users from accessing the targeted service, usually by overwhelming the target with superfluous requests.

[24] APT is a new type of cyber threat that uses "multiple attack techniques and vectors and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time." See Colin Tankard, "Advanced persistent threats and how to monitor and deter them," *Network Security* 11, no. 8 (2011): 16-19, https://www.sciencedirect.com/science/article/pii/S1353485811700861.

online to micro-target citizens with deeply personalized messaging. They will be able to exploit human emotions to elicit specific responses. They will be able to do this faster and more effectively than any human actor. Malicious actors—Russia or others—will use these technologies to their advantage. This transformation in digital communication is happening now—and the window for being able to detect the difference between human and machine-driven communications is closing.[6]

Weaponization of big data

During the 2016 U.S. election, Russia-linked accounts on Facebook published content on divisive social issues. The content had no ideological focus. Rather, the Russian strategy aimed to further incite polarization around hot political issues: race, immigration, religion, and gender. The accounts promoted the content using advertising tools readily available on Facebook and other social media to micro-target users who held similar beliefs. This content reached 150 million Facebook and Instagram users at a cost of only $100,000, according to congressional testimony by Facebook's general counsel in October 2017.[7] The Russian accounts were able to reach a large number of users at such low cost because Facebook and other tech firms' revenue models depend on their ability to collect increasingly refined personal data that make it possible for advertisers to micro-target individuals. In the hands of malicious actors, these data become a treasure trove for influence operations, political targeting, and manipulation.

[6] Matt Chessen, "The MADCOM future," (Washington, DC: Atlantic Council, September 2017), http://www.atlanticcouncil.org/publications/reports/the-madcom-future.

[7] "Hearing before the Committee on the Judiciary Subcommittee on Crime and Terrorism: Testimony of Colin Stretch, General Counsel, Facebook," Senate Judiciary Committee, October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf.

- ◦ **Credential reuse:** Obtaining valid credentials for one target and attempting to use those same credentials on other targets.

Examples

- **Democratic National Committee hack (United States, 2015-16):** U.S. intelligence agencies and private cybersecurity firms identified two groups—with ties to Russian intelligence—that were involved in the hacking of the Democratic National Committee (DNC). The hack led to a series of politically harmful emails being publicly leaked ahead of the U.S. presidential election. One group, APT 29 (or "Cozy Bear," or "The Dukes"), penetrated the DNC in July 2015 and was linked to the KGB's successor organization, the FSB.[25] The second, known as APT 28 (or "Fancy Bear"), hacked the DNC in March 2016 and had ties to the Russian Ministry of Defense's intelligence agency, the GRU. [26]
- **Bundestag hack (Germany, 2016):** Germany's domestic intelligence agency noted that hackers with ties to the Russian government had targeted both Chancellor Angela Merkel's political party and German state computers, which led to concerns that Russia would seek to disrupt the recent German elections.[27]

[25] Roland Oliphant, "Who are Russia's cyber-warriors and what should the West do about them?" *The Telegraph*, December 16, 2016, http://www.telegraph.co.uk/news/2016/12/16/russias-cyber-warriors-should-west-do/.

[26] Ibid.

[27] Kathy Gilsian and Krishnadev Kalamur, "Did Putin Direct Russian Hacking? And Other Big Questions," *The Atlantic*, January 6, 2017, https://www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/.

The threats involved with data collection are broader than the social media sector. An entire cottage industry of data brokers—companies that collect and sell individuals' personal data—has emerged to meet growing demand. Big data miners compile information from public records, web browsing histories, online purchases, and other sources. They use this information to predict tastes, political attitudes, ethnicity, place of residence, and other personal attributes. This information is just as valuable to companies marketing products to consumers as to foreign actors seeking to undermine democratic systems and authoritarian regimes (including Russia and China) seeking to control domestic populations. A 2014 study by the U.S. Federal Trade Commission (FTC) found that some companies collected as many as 3,000 pieces of information on a single consumer without the consumer's knowledge.[8] One such firm, Acxiom, claims to have collected data on 200 million Americans and reported revenues of $800 million in 2015.[9] Another firm, Cambridge Analytica, claimed to have created personal profiles on 240 million Americans.[10] The company mined personal data to micro-target voters in the United States during the 2016 election and in the United Kingdom during the Brexit referendum. These firms typically sell information to the highest bidder, but Cambridge Analytica reportedly contacted WikiLeaks in an effort to coordinate the leaks of Clinton's emails during the U.S. presidential election.[11] In December 2017, U.S. Special Counsel Robert Mueller requested that Cambridge Analytica turn over internal documents as part of his investigation into possible ties between the Trump campaign and Russia.[12]

Today, AI and personalized data that Twitter, Facebook, and others use to decide which content and ads appear in users' search results, newsfeeds, and timelines are already built into existing social media platforms. Social media companies can tweak their algorithms to better detect disinformation campaigns or other forms of manipulation (and they have begun to do so), but the underlying systems and revenue models are likely to stay the same. The coming threat is the development of AI and personalized data that Russia, China, and others will use to test and manipulate the existing systems.

Market demand for big data will continue to increase. Competition for advertising dollars incentivizes tech firms to collect more refined data about users, not less. In 2016, Facebook introduced emotional "interactions" on its platform, which allow users to react with an emoticon to a post. Now, rather than knowing what individuals like, this information allows malicious actors to know what type of content makes individuals happy, sad, or angry when such interactions (as Facebook calls them) are publicly shared by users. Armed with this information, any corporation, state, or non-state actor can devise a disinformation campaign that delivers content meant to incite an emotional response. For example, young unemployed white men who are likely to vote for a far-right political party in Germany would receive content suggesting that Syrian refugees are exploiting the

[8] Bridget Small, "FTC report examines data brokers," *Federal Trade Commission*, May 27, 2014, https://www.consumer.ftc.gov/blog/2014/05/ftc-report-examines-data-brokers.

[9] Brian Naylor, "Firms are buying, sharing your online info. What can you do about it?" *NPR*, July 11, 2016, https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it.

[10] Carole Cadwalladr, "British courts may unlock secrets of how Trump campaign profiled U.S. voters," *The Guardian*, September 30, 2017, https://www.theguardian.com/technology/2017/oct/01/cambridge-analytica-big-data-facebook-trump-voters.

[11] Rebecca Ballhaus, "Data firm's WikiLeaks outreach came as it joined Trump campaign," *The Wall Street Journal*, November 10, 2017, https://www.wsj.com/articles/data-firms-wikileaks-outreach-came-as-it-joined-trump-campaign-1510339346.

[12] Rebecca Ballhaus, "Mueller sought emails of Trump campaign data firm," *The Wall Street Journal*, December 15, 2017, https://www.wsj.com/articles/mueller-sought-emails-of-trump-campaign-data-firm-1513296899.

social welfare system or harassing German women. The post would call citizens to take undefined action.

This type of micro-targeted campaign is not a theoretical scenario; it is already happening and, when combined with more sophisticated AI, will only increase in its ability to predict deeply personal preferences and calibrate emotional responses. The layering of AI systems with the low-cost availability of personal data about individuals presents a serious challenge to democratic values of openness and free expression. With access to big data, AI systems will soon know us better than we know ourselves in terms of their ability to predict our political and personal preferences. Stanford computational data scientists, for example, have been able to create an AI system able to predict with 90 percent accuracy an individual's sexual orientation based on a photograph alone.[13]

Manufacturing "reality"

Russia's current disinformation model is premised on the concept of a "firehose of falsehood"—repetitive, fast paced, continuous, high-volume information attacks from a variety of sources.[14] The aim is to muddle the notion of truth or objectivity, blur the line between fact and falsehood, and sow confusion among publics. For now, this style of information war is detectable and easily debunked when found: doctored photographs can be revealed as fakes, videos claiming to show one event can be shown to actually reflect another, and quotes attributed to political leaders can also be fact checked. Civil society initiatives, such as Ukraine's StopFake.org, investigative journalists, such as First Draft News, and government agencies, such as the European External Action Service (EEAS) EastStratCom Team, have become much faster at monitoring, spotting, and debunking Russian efforts to spread this type of disinformation. Yet, with advances in techniques that can simulate human behavior, our ability to do so is quickly coming to an end.[15]

Discerning the difference between real and fake video or audio may be impossible in the very near term. New techniques in video and linguistic replication, driven by learning-enabled AI, are able to produce new video or audio recordings based on existing content. So-called "deep fakes," or the "digital manipulation of sound, images, or video to impersonate someone or make it appear that a person did something" are coming.[16] German and American researchers have been able to create believable video of an individual based on content from YouTube posts.[17] Audio is even easier to replicate. An AI program called Lyrebird "allows anyone to create his or her digital voice with only one minute of audio."[18] The implication of such new technologies is obvious: political leaders can be made to appear to say anything at all, and they will sound and look exactly as

[13] Yilun Wang and Michal Kosinski, "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images," *Journal of Personality and Social Psychology*, (2018, in press).

[14] Christopher Paul and Miriam Matthews, "The Russian 'firehose of falsehood' propaganda model: Why it might work and options to counter it," (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.

[15] Tim Hwang, "Digital disinformation."

[16] Robert Chesney and Danielle Citron, "Deep fakes: A looming crisis for national security, democracy, and privacy?" *The Lawfare Blog*, February 21, 2018, https://lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

[17] Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Niebner, "Face2Face: Real-time face capture and reenactment of RGB Videos," (paper presented at 2016 IEEE Conference on Computer Vision and Pattern Recognition, Seattle, WA, June 2016), http://www.graphics.stanford.edu/~niessner/papers/2016/1facetoface/thies2016face.pdf.

[18] "Lyrebird beta," Lyrebird, 2017, https://lyrebird.ai/.

they do in real life. These technologies stretch the definition of reality and fantasy. While these advancements are not inherently malicious in themselves, when put to use by bad actors, they can have detrimental effects on the media environment, public discourse, and public trust in mainstream institutions. If the viewers cannot trust their eyes and ears, confidence in media could plummet even further.

As deep fake capabilities become cheaper, faster, and more widely accessible, the "firehose of falsehood" model will become even more effective: videos of political leaders making derogatory remarks about their citizens could be pushed out on social media by thousands of bot and troll accounts. By the time that official sources are able to respond and debunk the hoax, new fake videos would already be going viral, and the accounts spreading the propaganda would appear to be very real and human. Using micro-targeted ads, the fake videos would reach the specific individuals and groups that are most likely to be offended. This cycle of disinformation would continue 24/7.

Cyberattacks on critical infrastructure

In the West, Russia's cyberattacks so far have been at the service of its disinformation operations: stolen data used to embarrass individuals, spin a narrative, discredit democratic institutions and values, and sow social discord. This was the pattern Russian operators followed in the United States, France, and Germany during the countries' 2016-17 elections. Hacking email accounts of individuals or campaigns, leaking that stolen information via a proxy (primarily WikiLeaks), and then deploying an army of disinformation agents (bots, trolls, state-controlled media) to disseminate and amplify a politically damaging narrative.[19] Such cyber-enabled interference falls below the threshold of "cyberattacks of significant consequence" that could result in "loss of life, significant destruction of property, or significant impact on [national security interests]."[20] Partially for this reason, Western governments, which have been the targets of cyber-driven information war, have not responded in a decisive and visible manner.

In the West, the nightmare of cyberattacks crippling critical infrastructure systems—electricity grids, hospitals, financial systems, transportation—still has the sound of science fiction. But in Europe's East, this nightmare scenario is a reality, and a sign of what is very likely to come in Europe and elsewhere.[21] As the laboratory for Russian activities, Ukraine has seen a significant uptick in attacks on its critical infrastructure systems since the 2013-14 Maidan revolution. A barrage of malware, denial of service attacks, and phishing campaigns bombard Ukraine's critical infrastructure environments on a daily basis.

In December 2015, a well-planned and sophisticated attack on Ukraine's electrical grid targeted power distribution centers and left 230,000 residents without power the day before Christmas. The attackers were able to override operators' password access to

[19] On Germany's experience with Russian cyberattacks since 2015, see Tyson Barker, "Germany strengthens its cyber defense," *Foreign Affairs*, May 26, 2017, https://www.foreignaffairs.com/articles/germany/2017-05-26/germany-strengthens-its-cyber-defense. On the #MacronLeaks disinformation campaign, see "Hashtag campaign: #MacronLeaks," *DRFLab*, May 5, 2017, https://medium.com/dfrlab/hashtag-campaign-macronleaks- 4a3fb870c4e8. For a review of Russian disinformation efforts in Germany, see Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," *Brookings Institution*, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[20] "The DoD cyber strategy," (Arlington, VA: Department of Defense, 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[21] Andy Greenberg, "How an entire nation became Russia's test lab for cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

the system and also disable backup generators. Thanks to Soviet-era manual switches, the blackout lasted only a few hours and thus went almost unnoticed in the West. The Ukrainian government attributed the attacks to the Russian Advanced Persistent Threat (APT) group "Sandworm."[22] "BlackEnergy," the same Sandworm malware that caused the blackout in Ukraine, has been detected in electric utilities in the United States.[23] The Christmas attack is the worst known attack on critical infrastructure systems, and Ukraine's systems—defended by a combination of firewalls, segmented access, two-factor authentication, and manual controls—were more secure at the time of the attack than those in the United States.[24]

Attacks on Ukraine and other Eastern European countries are not always easily contained. In June 2017, the so-called "NotPetya" virus, which originated in a targeted attack on Ukraine's accounting systems, spread to 64 countries and affected major international companies, logistical operators, government agencies, telecommunication providers, and financial institutions. The name, NotPetya, referred to the disguised nature of the attack; it appeared as a previously launched ransomware attack (Petya) but was in fact designed to destroy and delete information systems in Ukraine.[25] In effect, NotPetya was a cyber form of "*maskirovka*"—tactical deception—used in Soviet military operations to mislead and deceive adversaries about the true source and intention of an attack. In February 2018, the U.S. administration attributed NotPetya to the Russian military.[26]

> NotPetya was a cyber form of '*maskirovka*'—tactical deception—used in Soviet military operations to mislead and deceive adversaries about the true source and intention of the attack.

Ukraine's experience with Russian election hacking should also be a call to action. Widely used electronic voting machines have weak security and software full of easily exploitable loopholes. At the 2017 Defcon conference for hackers, attendees were tasked with breaking into a range of American voting machines either by finding vulnerabilities through physically breaking into machines or gaining access remotely. The hackers did so in less than two hours.[27] Participants managed to breach every piece of equipment by the end of the gathering.[28]

A massive and debilitating attack on critical infrastructure in Western Europe and the United States is inevitable. It will likely follow a pattern similar to the May 2017 WannaCry ransomware attack that crippled hospitals in Western Europe by exploiting a vulnerability in Microsoft Windows. The exploit was originally identified by the NSA and was

[22] Kim Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," *Wired*, March 3, 2017, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[23] Andy Greenberg, "How an entire nation became Russia's test lab for cyberwar."

[24] Ibid.

[25] Frank Bajak and Raphael Satter, "Companies still hobbled from fearsome cyberattack," *Associated Press*, June 30, 2017, https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2/Companies-still-hobbled-from-fearsome-cyberattack.

[26] "Statement from press secretary," The White House, February 15, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

[27] Barb Darrow, "How hackers broke into U.S. voting machines in less than 2 hours," *Fortune*, July 31, 2017, http://fortune.com/2017/07/31/defcon-hackers-us-voting-machines/.

[28] Matt Blaze et al., "Defcon 25 voting machine hacking village: Report on cyber vulnerabilities in U.S. election equipment, databases, and infrastructure," (Defcon, September 2017), https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

subsequently leaked. The Shadow Brokers, a hacker group, published the information from the National Security Agency (NSA) leak containing the information about the vulnerability in April 2017. The United States identified North Korea as responsible for the WannaCry attack in the fall of 2017.[29] WannaCry presents a clear threat vector: malicious actors (Russia, China, North Korea, etc.) hack Western intelligence agencies' tools and post them publicly, allowing other malicious actors around the world to attack critical infrastructure. And the West seems ill-equipped to deter and respond to such an event.[30]

GETTING AHEAD OF THE GAME: A TRANS-ATLANTIC RESPONSE

Russia may present a template for political warfare today, but it is already yesterday's game. As existing tools and methods are exposed and countered, and technology continues to advance and become more financially accessible, malicious actors will continue to evolve their tactics. The short-term emerging threats described in this paper are just a sample of what is to come. The time horizon of three to five years may be too generous and the threat even more imminent.

> **Russia may present a template for political warfare today, but it is already yesterday's game.**

A reactive policy approach that simply plugs the gaps of existing vulnerabilities, or responds on a case-by-case basis, will fail. The threat is bigger than Russia and broader than any single nation-state actor: it is a challenge to trans-Atlantic security, democratic values, and the entire international system. A policy to counter and deter future threats must be trans-Atlantic in scope, future-facing, and inherently collaborative. A democratic response to political warfare against the West is possible, but it will require a whole-of-society, multi-stakeholder approach. Governments, multilateral institutions, civil society, the private sector, and individual citizens must all play a part. To survive and thrive in the next great leap in political warfare, the immediate response should take shape along three lines of effort:

1. Information sharing

- *European governments, the United States, and allies should establish information sharing mechanisms with private sector firms.* As Google, Facebook, and Twitter stated in U.S. congressional testimonies in the fall of 2017, they do not wish to be manipulated by actors aiming to undermine democracies. As such, these tech firms should voluntarily cooperate with public sector agencies, particularly the intelligence community, to establish an early warning system when disinformation activities are detected in their systems. To that end, national governments, the European Union, and NATO should establish a designated interlocutor within the intelligence agencies to be the point of contact for receiving and distributing such information, as appropriate. A voluntary information sharing system is ideal, but such processes could also be legislatively mandated.

[29] Thomas P. Bossert, "It's official: North Korea is behind WannaCry," *The Wall Street Journal*, December 18, 2017. https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

[30] Susan Hennessey, "Deterring cyberattacks," *Foreign Affairs*, December 4, 2017, https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks.

- *NATO, the European Union, and the United States should establish an information sharing unit focused specifically on cyber-enabled disinformation.* NATO, as the primary defense and security organization linking the trans-Atlantic partnership, should take the lead in coordinating information sharing through existing and new mechanisms in NATO's Cyber Command or NATO's Joint Intelligence and Security (JIS) Division.

- *European governments and the United States should convene, on a regular basis, the StratCom, Hybrid Threat, and Cyber Threat task forces that currently exist within various agencies.* Task forces such as the EEAS's EastStratCom team, the Czech Ministry of Interior's StratCom Unit, the joint European Center of Excellence for Countering Hybrid Threats in Helsinki, and NATO's StratCom Center of Excellence in Riga, among others, should develop closer relationships through regular convening and information sharing. An annual StratCom forum should be established in Brussels under the auspices of the European Council but with participation from the United States and allies.

2. Improve information security and transparency

- *European states and the United States should order an immediate audit of governmental information systems, network security, and classified systems.* Such a review should identify immediate vulnerabilities while also looking forward to emerging threats. The resulting report should be classified, but should have an unclassified version to inform the public. Such an audit should be completed quickly and its recommendations taken seriously.

- *Private sector tech and social media firms should develop tools to quickly identify fake and automated accounts.* Early attempts to label potentially disputed content have not succeeded in deterring users from clicking on such content.[31] De-ranking or "muting" such content is likely to be more effective.

- *Private sector firms should vet advertising clients to prevent malicious actors from promoting content.* Known propaganda culprits should be banned from advertising on social media platforms (an action already taken by Twitter) and their content should be pushed down in the ranking (an action Google has said that it would take).

- *Private sector tech firms should agree to a corporate code of conduct regarding advertising and data.* Among other rules, it would limit the detail of personal data used in advertising tools, introduce transparency into ad revenue streams, and extend the restrictions around political advertising already in place for traditional media into the online space.

- *Data brokers should be required by law to give consumers access to their data, including the ability to correct it.* Consumers should also be prominently notified by social media platforms and other retailers when their data are being shared with data brokers.

- *Academic institutions training the next generation of computer scientists should introduce ethics courses into the required curriculum.* Algorithms are written

[31] Catherine Shu, "Facebook will ditch disputed flags on fake news and display links to trustworthy articles instead," *TechCrunch*, December 20, 2017, https://techcrunch.com/2017/12/20/facebook-will-ditch-disputed-flags-on-fake-news-and-display-links-to-trustworthy-articles-instead/.

by humans and thus have inherent biases built into them. So-called "neutral" algorithms are an illusion. More awareness of the potential ethical implications of computer coding could make algorithms and AI less susceptible to manipulation.

3. Invest in research and development on AI and computational propaganda

- *Governments, private foundations, major non-profit policy organizations, and technology companies should invest in academic research that explores how technological advances will affect public discourse.* While AI technology will positively transform many sectors—health, transportation, and others—the potential negative implications of new technologies should also be acknowledged and researched.

- *To get ahead of machine-driven computational propaganda, technology companies (current and future) should develop the next generation of AI-driven detection techniques and build them into platforms before the threat becomes more urgent.* This will mitigate the possibility of malicious actors manipulating online platforms in the future.

- *Governments, private foundations, academia, and tech companies should invest in research that examines the "demand side" of disinformation in addition to the "supply side."* Disinformation narratives spread because individuals find them appealing. The techniques and tools are just one side of the equation. Better understanding the social psychology of disinformation would help governments, independent media, and civil society groups become better equipped to counter such messaging.

THE LONG VIEW: IS DETERRENCE AGAINST POLITICAL WARFARE POSSIBLE?

Deterrence as a conventional military strategy depends on one actor's ability to dissuade another from taking a damaging action through intimidation and coercion. For a deterrent to be effective, the adversary must understand the consequences of carrying out an offensive action and believe in the credibility and ability of the other side to impose the consequences. For example, during the Cold War, both the Soviet Union and the United States knew what the consequences of a pre-emptive nuclear strike would be—imminent mutual destruction.

In nonconventional warfare, however, the consequences and implications of an offensive action are ambiguous to both sides. The Obama administration, for example, did not have a clearly defined response strategy to Russian interference in the 2016 presidential election. Eventually, in the final months of his presidency, Obama signed an executive order imposing cyber-related sanctions on Russia, expelled 35 Russian diplomats from the United States, and seized two Russian diplomatic compounds. These actions were not commensurate with the scale of the Russian attack. In its first year, the Trump administration has not developed a comprehensive strategy either, while the president continued to question the scope of Russian activities. It is likely that the Russian government also did not know what to expect in response to the disinformation and cyber operations it carried out. Moscow was testing U.S. resolve to respond. The weakness of the U.S. response has undoubtedly been a useful lesson for other states—China, Iran, North Korea—seeking to undermine Western societies.

As a first step, *Western governments should develop a strategy of deterrence against political warfare with clearly defined consequences for specific offensive actions*. This strategy should have overt and covert operational components, including public statements by high-level government officials that outline the consequences, intelligence communications to convey the potential costs to adversaries, and an increase in covert operations aimed at identifying adversaries' vulnerabilities.

Nonconventional deterrence is difficult for another reason: attribution. The Russian government continues to deny any involvement in the U.S. and European elections. The 2017 unclassified U.S. intelligence report on Russian interference stopped short of laying the blame explicitly on President Putin, despite overwhelming evidence that the direction for such an operation had to come from the highest office of the Russian government. The German government took a different approach in the lead-up to the federal elections in September 2017. Most notably, in May 2017, the head of the German intelligence service, the BfV, publicly warned the Kremlin from making the political decision to interfere.[32] Chancellor Merkel warned the German public of possible Russian interference directly after the U.S. election in November 2016. These public warnings from high-level officials likely impacted the Kremlin's decision to not leak data obtained in a 2015 hack of the German parliament.[33] The goal of political warfare is to conceal the perpetrator and maximize plausible deniability. *Western political leaders should not fall victim to adversaries' obfuscation techniques, but rather take a principled public stance on attribution.* Such warnings must come from trusted messengers and from the highest level of government.

Lastly, a warning: in seeking to deter political warfare, Western democracies cannot abandon the core values of openness, freedom of expression, and liberalism. Regulatory initiatives for better transparency and accountability in the social media space are important, but regulation must not devolve into infringements on freedom of expression. Democratic governments cannot beat malicious state actors at their own game: a top-down approach that involves the spread of counter-propaganda will only erode the remaining trust that citizens have in government institutions. Fighting propaganda with propaganda is also not the way forward. A democratic response must be rooted in civil society and an independent media. A multi-stakeholder approach—in which individuals, governments, civil society organizations, and private firms play their part—is a strength, not a weakness, of democracies.

[32] Lizzie Dearden, "German spy chief warns Russia cyber attacks aiming to influence elections," *The Independent*, May 4, 2017, http://www.independent.co.uk/news/world/europe/germany-spy-chief-russian-cyber-attacks-russia-elections-influence-angela-merkel-putin-hans-georg-a7718006.html.

[33] "Bundestag counting cost of cyberattack," *Deutsche Welle*, June 11, 2015, http://www.dw.com/en/bundestag-counting-cost-of-cyberattack/a-18512512.

ABOUT THE AUTHORS

Alina Polyakova is the David M. Rubenstein Fellow in the Brookings Institution Foreign Policy program's Center on the United States and Europe, and adjunct professor of European studies at the Paul H. Nitze School of Advanced International Studies at Johns Hopkins University. Polyakova's writings have appeared in *The New York Times*, *The Wall Street Journal*, *Foreign Affairs*, *Foreign Policy*, and *The Atlantic*, as well as a number of academic journals. Her book, *The Dark Side of European Integration* examines the rise of far-right political parties in Europe. Prior to joining Brookings, Polyakova served as director of research and senior fellow for Europe and Eurasia at the Atlantic Council. Polyakova holds a doctorate from the University of California, Berkeley.

Spencer P. Boyer is currently a Nonresident Senior Fellow in the Brookings Institution Foreign Policy program's Center on the United States and Europe and an adjunct professor at Georgetown University's School of Foreign Service. From 2014-17, he was the national intelligence officer for Europe in the U.S. National Intelligence Council. During the first term of the Obama administration, he served as a deputy assistant secretary of state for European and Eurasian Affairs. He has been a senior analyst or visiting scholar with numerous think tanks, including the Center for American Progress, the Center for Transatlantic Relations at the Johns Hopkins School of Advanced International Studies, and the Woodrow Wilson International Center for Scholars.

ACKNOWLEDGEMENTS

This paper was made possible by funding from the Robert Bosch Stiftung.

The authors would like to thank the following individuals for their feedback, comments, and assistance on drafts: Natalie Britton, Sinan Ekim, Jakub Janda, James Lamond, Filippos Letsas, Chris Meserole, Ted Reinert, Rachel Slattery, Tom Wright, Anthony Yazaki, and the anonymous reviewers who provided additional guidance.

This publication is part of the Brookings – Robert Bosch Foundation Transatlantic Initiative (BBTI), a comprehensive multi-year project of applied research and programming aimed to create synergies and originate new activities that reinvigorate transatlantic collaboration on global issues. Brookings recognizes that the value it provides is in its absolute commitment to quality, independence, and impact. Activities supported by its partners reflect this commitment. The conclusions and recommendations of any Brookings research are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu