Policy Blueprint for Countering Authoritarian Interference in Democracies

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

POLICY BLUEPRINT FOR COUNTERING AUTHORITARIAN INTERFERENCE IN DEMOCRACIES

2018 | No.27

JAMIE FLY, LAURA ROSENBERGER, AND DAVID SALVO

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

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

About the Authors

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

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

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

About the Alliance for Securing Democracy

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

About GMF

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

Photo Credits: Unsplash.com/ Shutterstock.com

Executive Summary

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

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

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

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

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

A New Strategic Approach for Government and Society

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

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

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

Recommendations

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

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

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

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

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

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

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

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

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

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

5. Make transparency the norm in the tech sector.

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

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

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

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

8. Increase support for local and independent media.

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

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

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

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

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

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

Foreward

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I. The Operation against America

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21 U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Majority Staff Report: Russian Attempts to Influence U.S. Domestic Energy Markets by Exploiting Social Media, March 1, 2018, 115*th Cong., 2nd sess., https://science.house.gov/sites/republicans.science.house.gov/files/documents/SST%20Staff%20Report%20-%20Russian%20Attempts%20to%20Influence%20U.S.%20Domestic%20Energy%20Markets%20by%20Exploiting%20Social%20Media%2003.01.18.pdf.

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

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

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

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

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

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

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

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

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

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

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

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

30 Ibid.

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

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

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

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

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

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

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

32 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets As Sources For Partisan Opinion: Study," *Columbia Journalism Review, March 8, 2018,* https://www.cjr.org/analysis/tweets-russia-news.php.

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

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

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

The Asymmetric Toolkit

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

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

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

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

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

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

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

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

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

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

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

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

An Overview of Russia's Asymmetric Operations in Europe

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

55 Mike Corder, "Netherlands, Austria Hold Russia Liable for Downing MH17," *The Associated Press, May 25, 2018,* https://apnews.com/4b05cd0e43c84e74822ebf1356337cdf; "Defensive Disinformation as Decoy Flare: Skripal and Flight MH17," *EU vs Disinfo, March 27, 2018,* https://euvsdisinfo.eu/defensive-disinformation-as-decoy-flare-skripal-and-flight-mh17/.

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

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

III. A New Strategic Approach for Government and Society

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

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

Whole of Government

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

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

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

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

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

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

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

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

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

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

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

Raising the Cost on Our Adversaries

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

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

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

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

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

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

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

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

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

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

A Transatlantic Threat Demands a Transatlantic Response

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

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

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

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

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

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

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

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

Whole of Society Approach

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

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

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

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

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

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

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

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

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

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

An Urgent Call to Action to Secure Democracy

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

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

IV. Recommendations for the U.S. Government

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

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

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

The Administration should:

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

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

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

Congress should:

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

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

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

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

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

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

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

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

The Administration should:

- Maintain the designation of electoral systems as critical infrastructure.

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

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

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

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

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

Congress should:

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

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

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

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

- Enact requirements for the federal government to notify states and relevant local election officials of intrusions into electoral infrastructure, and for the Executive Branch to notify Congress — both in a timely manner. Legislation should also require private vendors and operators of electoral infrastructure to report cybersecurity incidents that could impact the integrity of voting systems and databases to the FBI and DHS.

- Require DHS to issue security clearances to senior state government officials in charge of securing electoral infrastructure in order to facilitate access to information on threats.

- Codify into law the designation of electoral systems as critical infrastructure.

- Prioritize federal funding for cybersecurity research and development.

- Pass legislation to elevate the DHS National Protection and Programs Directorate into a full-fledged operational agency under DHS jurisdiction; one bill has already been introduced and is being considered by Congress.[68] The agency should facilitate improved coordination across government on responses to cyber threats to all 16 critical infrastructure sectors.

State and local governments should:

- Accept federal assistance on election security. While it is not a federal government competency to run elections, states lack the resources and expertise that the federal government possesses on cyber threats to critical infrastructure.

- Comply with EAC's voluntary voting system guidelines and the National Institute of Standards and Technology's cybersecurity framework for critical infrastructure.

- Make mandatory the use of electronic voting machines that issue a voter verified paper ballot, and the conduction of post-election audits of paper voting records to corroborate electronic results.

- Conduct an audit and threat analysis of voter registration systems, and upgrade systems as necessary, as recommended in a Brennan Center for Justice report.[69]

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

NSC Foreign Interference Coordinator

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Administration should:

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

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

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

Congress should:

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

- Pass legislation to have bots identified and labeled.

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

V. Recommendations for the European Union and NATO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VI. Recommendations for the Private Sector

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VII. Recommendations for Media Organizations[87]

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

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

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

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

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

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

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

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

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

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

89 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets As Sources For Partisan Opinion: Study," *Columbia Journalism Review, March 8, 2018,* https://www.cjr.org/analysis/tweets-russia-news.php.

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

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

- Using timelines and network diagrams to map out key players and events in multilayered stories.

- Create a dedicated vertical to a theme that encompasses many high-profile and breaking articles, such as Russian interference in democracies. This would put all relevant stories in one location for users to find information.

- Break down complicated stories by using Q&As and explainer cards.

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

- Participate in The Trust Project, a new initiative that is developing transparency standards for news consumers to assess the quality and credibility of journalism. Journalists would explain why they wrote a particular story, sources they used, previous versions of the story, etc.

- Require freelancers to disclose their sources of funding and any possible conflicts of interest. This will help prevent manipulation of freelancers and could weed out fake freelancers.

- Write stories about journalistic procedure. In other words, explain to the public how journalists do their jobs. Entire TV series have been devoted to shedding light on a profession. Public interest stories on a reporter's approach to a particular story or source could generate interest in the news outlet while simultaneously increasing transparency.

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

- Assign responsibility for disinformation and emerging threats to a C-level executive within the news organization. The executive would be in charge of finding solutions to verify potentially falsified information.

- Create a regular schedule for revisiting and updating social media verification guidelines.

- Follow BuzzFeed's lead and assign a beat reporter to cover disinformation trends and technologies to keep its audience updated on the latest developments.

VIII. Recommendations for Civil Society

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

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

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

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

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

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

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

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

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

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

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

Acknowledgements

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

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

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

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

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

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

Appendix A: Influential Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix B: ASD Advisory Council

Mike Chertoff

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

Toomas Ilves

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

David Kramer

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

Bill Kristol

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

Rick Ledgett

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

Michael Morell

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

Mike McFaul

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

Mike Rogers

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

Kori Schake

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

Julie Smith

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

Admiral Jim Stavridis (Ret.)

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

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

Jake Sullivan

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

Nicole Wong

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

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

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

www.gmfus.org