Policy Blueprint for Countering Authoritarian Interference in Democracies

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

alliance for securing democracy
G|M|F

Executive Summary

2018

The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies

By Jamie Fly, Laura Rosenberger, and David Salvo

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- Insufficient cyber defenses and outdated electoral infrastructure;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

Executive Summary

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. 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

Executive Summary

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 cyberattacks 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 cyber-attacks 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 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.

Executive Summary

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.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Authors

Laura Rosenberger is director of the Alliance for Securing Democracy at The German Marshall Fund of the United States.

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, where he is also co-director of the Alliance for Securing Democracy.

David Salvo is deputy director of the Alliance for Securing Democracy at The German Marshall Fund of the United States.

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 does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, nonprofit 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.

1700 18th Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.securingdemocracy.org/