FEBRUARY 2018

Countering Adversary Threats to Democratic Institutions

An Expert Report

PRINCIPAL AUTHOR
Suzanne E. Spaulding

CONTRIBUTING AUTHOR
Eric Goldstein

FOREWORD
John J. Hamre

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

FEBRUARY 2018

Countering Adversary Threats to Democratic Institutions

An Expert Report

PRINCIPAL AUTHOR
Suzanne E. Spaulding

CONTRIBUTING AUTHOR
Eric Goldstein

FOREWORD
John J. Hamre

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship has contributed to its publication.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

Participants and Contributors

The titles and affiliations of the following participants and contributors appear in Annex A.

John Bellinger

Meryl Chertoff

Michael Chertoff

Matt Chessen

Frank Cilluffo

David S. Cohen

Heather Conley

Mary DeRosa

Joseph P. Federici

Michèle Flournoy

Geyshia Gonzalez

Siobhan Gorman

Ken Gude

John Hamre

Michael Hayden

David Heyman

Nina Jankowicz

James Lewis

John MacGaffin

Holly McMahon

Jeffrey Rathke

Harvey Rishikof

Eric Rosenbach

Laura Rosenberger

Paul Rosenzweig

David Sanger

Loren Shulman

Suzanne E. Spaulding

Neal Wolin

Foreword

American democracy is under attack from Russia. This is a long-term campaign that did not begin or end with the 2016 election. Putin's objective is to weaken us by sowing chaos and discord, and to undermine the appeal of democracy itself. If he can show that American-style democracy, both in the United States and in other liberal democracies, is incompetent, illegitimate, and hypocritical, he can use that narrative to undermine its potential appeal among Russia's population and in other countries around the world where we compete for influence. Other nations with similar interests are likely to follow suit, waging their own campaigns against democratic institutions.

Cognizant of this threat, a bipartisan group of experts gathered at the Center for Strategic and International Studies (CSIS) in late spring of 2017 to share their insights and discuss ways to counter Russia's efforts to undermine fundamental democratic institutions. This report is informed by that discussion, as well as a subsequent roundtable in December and other expert input. It provides some background on Russia's playbook, as seen in Eastern and Central Europe primarily, and how those tactics were used in the United States in 2016 and continue today. It highlights the role of technology in facilitating democratic disruption, including network intrusions and exploitation of social media. With the growing sophistication powered by machine learning, enabling even convincing fabrication of speech and video, distinguishing between truth and disinformation will become increasingly difficult.

Russian influence operations exploit vulnerabilities of our own making, both cyber vulnerabilities and societal vulnerabilities. They fan the flames of existing divisions and skepticism, sometimes jumping in on both sides of an issue, as in the debate about racial justice. As they exacerbate tensions and divisions, they take aim at pillars of democracy. Their targets go beyond the executive branch to include the Congress, the justice system, and the media.

The bipartisan Experts Group that gathered at CSIS in the spring and winter of 2017 concluded that we need a whole-of-nation strategy to counter foreign adversary attacks on these fundamental institutions of democracy—and we need it now. Ongoing investigations in Congress and by the special prosecutor may continue to reveal new details about Russian tactics. However, we know enough now to understand that the attacks did not stop last November and there is an urgent need to more effectively counter them. Efforts are underway outside of government, and some of those are captured in this report. What is needed is a national approach that pulls together governments, at all levels in the United States and with like-minded nations around the globe, along with civil society, academia, technology companies, and the public.

Informed by the Experts Group, this report outlines just such a national strategy designed to prevent, deter, and reduce the effectiveness of active measures targeting democratic

institutions. It calls for a whole-of-nation campaign to enlist all Americans in this essential struggle to combat an adversary bent on weakening our nation.

John J. Hamre
President & CEO
CSIS

01

Introduction

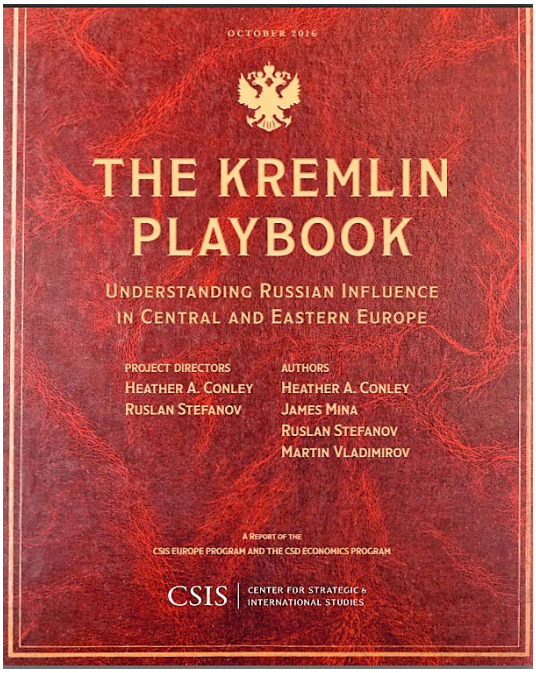
This report, informed by the two Experts Group roundtables listed in Annex A, proceeds in four sections. First, the report outlines the nature of the threat posed by the Russian government, building upon what Russia has done in other countries as well as in the United States. The second section describes how technology has magnified this threat. The third section examines essential elements of a *National Strategy to Counter Russian and Other Foreign Adversary Threats to Democratic Institutions*. The final section is a call for action.

02

Reviewing the Playbook: The Nature of the Current Threat

Russia is engaged in a determined assault on Western democracies and their institutions. The intelligence community assessed that efforts to influence the U.S. election were part of the Kremlin's "longstanding desire to undermine the U.S.-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin's regime." Putin aims to "discredit the image of the United States and cast it as hypocritical." Its military doctrine of New Generation Warfare is "... primarily a strategy of influence, not of brute force...[but of] breaking the internal coherence of the enemy system." The Kremlin's strategy of influence is well documented in the 2016 research findings of the CSIS report *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*.

Although Russian interference in democratic electoral processes, particularly in the country's "near-abroad," has been recognized for more than a decade, activities surrounding the 2016 U.S. election, and continuing to the present day, differed in both degree and kind. While past election meddling in Russia's near-abroad focused on changing the results of an individual election through tactics such as financial support or organized elections violations, in the United States the Russian government invested in a systematic, multiyear campaign to not merely affect the results of an individual election, but sow chaos and undermine trust in the liberal democratic order itself. At the same time, Russia has exploited technological innovations, particularly mass communications platforms such as Twitter and Facebook, to multiply the impact of its activities and cause previously infeasible effects.



...many of the influence techniques seen in the U.S. election are similar to those Russia has employed elsewhere.

Expert participants at the CSIS roundtable observed that many of the influence techniques seen in the U.S. election are similar to those Russia has employed elsewhere, in different contexts. To advance its goals across disparate regions, particularly in Eastern and Central

Europe, the Russian government has followed a multipart strategy of economic influence, state capture, disinformation, and developing affinity groups. While techniques, tactical objectives, and expectations applicable to the United States may differ, outlining the Kremlin's playbook elsewhere offers important lessons.

Economic Influence/State Capture

In the first instance, the Russian government has advanced its strategic influence in Eastern and Central European countries by gaining influence, and in some instances, control over specific sectors: energy, banking and finance, real estate, transportation infrastructure, and media, following the same general process across multiple countries. The Experts Group was briefed on a multistep approach repeatedly executed by the Russian government in nations from Hungary to Ukraine. First, Russian state-owned enterprises purchase assets in the target nation. The purchased entity then gains influence with local officials, ostensibly to protect their economic investment. As the purchased entity becomes increasingly profitable, its political influence with government officials increases apace. Simultaneously, the Russian government creates or fosters local nongovernmental organizations (NGOs) to promulgate a sympathetic narrative about the Russian-owned companies and the Russian state more generally. Finally, supportive local officials are placed in national governments and given oversight, anticorruption, and national security portfolios, where they further stymie negative coverage or countervailing efforts by anticorruption officials and activities. Collectively, these activities in some countries result in state capture.

Information Operations

State capture of the kind seen in Eastern Europe requires specific conditions, including a significant level of investment and exploitation of weaknesses in national institutions, particularly the judiciary and anticorruption bodies. The Russian government has developed alternative mechanisms to exert influence where state capture is presently infeasible or impractical. The Experts Group focused particularly on the threat of information operations that can be executed with minimal resources by proxy entities using transnational communication platforms.

[In Eastern Europe, Russia exploits] weaknesses in national institutions, particularly the judiciary and anticorruption bodies.

The Russian government engages in numerous information operations that support a common overarching goal: to erode trust in Western governments and sow confusion and discord among target populations. During the 2016 U.S. election, this broader strategic goal was supplemented by the objective of targeting the residential campaign of Hillary Clinton, for whom Putin had a special dislike. Moreover, one participant noted the importance of recognizing that Russian leadership may be executing information operations, in part, in retaliation for what it believes is a U.S.-led plot to undermine its legitimacy, ostensibly exemplified by the 2005 Orange Revolution and 2014 Euromaidan protests and subsequent revolution in Ukraine, the release of the Panama Papers, and the disqualification of many Russian athletes from the 2016 and 2018 Olympics.

Russia's information operations in the United States and elsewhere generally fall into two categories. First, individuals operating under the direction of the Russian government leverage social and mass media platforms to foster specific narratives intended to advance political objectives or simply introduce further divisiveness into the political discourse, along with more nuanced messaging to support affinity groups. These activities are reinforced by the use of "bots," automated programs that expand and amplify social media messaging. Second, messaging on social and mass media platforms is fueled by information gleaned by hacking of government institutions, media, and political parties. This stolen information is used to further bolster the desired narratives through systematic leaks.

The 2016 presidential election was confronted with perhaps the most sophisticated and pervasive information operation campaign ever perpetrated, including widespread messaging campaigns on Facebook and Twitter leveraging stolen information from political parties and representatives. In the last year, Russia has engaged in similar activities in democratic elections throughout Europe.

Did you see Russian Information during the 2016 campaign?

- 126 million people saw free posts made by 470 Russian accounts and pages affiliated with the Russian Internet Research Agency.
- 10 million saw ads paid for by Russian accounts.
- Russian operatives used Facebook to publicize 129 phony event announcements, drawing the attention of nearly 340,000 users—many of whom said they were planning to attend.

Hearing, U.S. Senate Select Committee on Intelligence, November 1, 2017

Of significant concern is the potential for Russian operations to undermine confidence in the election process and its result. As recently as January 29, 2018, Central Intelligence Agency Director Mike Pompeo said he has "every expectation" the Russians will try to meddle in the 2018 midterm elections.

Russian activity targeting systems containing voter registration data, for example, raised the possibility that rolls would be corrupted in ways that could disrupt voting, causing long lines and voters being sent to wrong polling places, and thereby undermine confidence in the process and, potentially, the outcome. Other cyber-enabled disruptions, such as to media analysis and reporting on results, could have similar effects.

The same kinds of techniques could be used to undermine public confidence in other fundamental institutions of democracy, including America's justice system. Cyber attacks on critical infrastructure or intrusions into systems within the three branches of government could similarly undermine confidence in the U.S. government and further sow chaos and division. For example, the use of malicious cyber activity that clearly impacts data confidentiality, access, or reliability, as well as attacks on industrial control systems, could be used to directly advance a

Russian-promoted narrative about incompetence, hypocrisy, or corruption of government officials.

Drive wedges deeply enough, and you undermine the sense of shared values that forms the foundation of democracy.

The broader effort to exacerbate existing divisions in society is also a way to weaken democracy. Russian-affiliated social media activities have been detected on both sides of the racial justice debates, for example. They have amped up the volume on both sides of the "take a knee" controversy in the NFL, and set up fake activist groups such as *Black MattersUS* and *Blacktivitst*. They have also stoked the flames of controversy around immigration and refugees, going so far as to invent protests and invite readers to attend. Drive wedges deeply enough, and you undermine the sense of shared values that forms the foundation of democracy.

> "Russian-linked accounts continued their assault on the U.S. justice system by seeding Twitter with a steady diet of content meant to undermine faith in the rule of law. Close to half of the top URLs promoted by the network pushed deep state narratives, including Uranium One, the Fisa memo, attacks against Pete Strzok and the Mueller investigation, and various conspiracy theories. Since the launch of the dashboard, content focused on undermining law enforcement and the Justice Department has increased steadily, suggesting an attempt not only to divide Americans but to erode faith in our systems of government."
>
> *Securing Democracy Dispatch*, February 12, 2018, https://sites-gmf.vuturevx.com/113/3699/february-2018/asd-newsletter-(new)(4).asp?sid=4075879b-eb58-4207-8702-ef0b70bc6ba9.

Building Affinity Groups

The creation of "affinity groups" is a common element of Russian information operations. For example, the Experts Group discussed the perception of Russia as the "3rd Rome" among an increasingly broad constellation of groups and individuals. Russian nationalists, with the encouragement of the Russian government, have promoted the idea of Russia as the heir to the Byzantine and Roman empires. This viewpoint emphasizes the alleged degradation of "Western" values, generally defined in terms of racial and ethnic purity, throughout Europe and the United States. Among these entities, which generally identify with the far-right wings of their domestic political spectrum, Russia is the sole protector of "legitimate" conservative values: homophobia, xenophobia, and anti-Semitism. The Experts Group discussed the extent to which the Russian government provides such groups with messaging, platforms, and validity in lieu of overt support. The group particularly noted the role of affinity groups in the 2017 French election, in which rumors about then-candidate Emmanuel Macron were channeled through U.S-based organizations, although it is not clear this was an effective tactic and may even have backfired.

03

Shifts in the Landscape: Technological Mediation of Democratic Disruption

Russian interference in fundamental institutions of democracy is not a new phenomenon. However, technological innovation has vastly increased the scope and efficacy of disruptive efforts. In addition to cyber-enabled disruption, the Experts Group examined the need to address the exploitation of social and mass media platforms, as occurred during the 2016 election, while taking immediate steps to confront emerging technologies that will become increasingly salient in the near future. The group noted the need to address the prevalence of bot-enabled information operations on major social platforms, particularly in the context of rapid advances in "computational propaganda."

In the near term, the Experts Group discussed the importance of online disinformation campaigns affecting the narrative around specific national elections and influencing public discourse generally. Examples of this latter phenomenon are automated bots stirring the pot on divisive issues like racial justice and refugees.

Critically, and highlighting an area for future research, several of the assembled experts noted that it is presently unclear whether automated bots are protected by the First Amendment of the U.S. Constitution; that is, whether an individual's right to free speech extends to the output of a computer program that the individual created. The Russians appear aware that this kind of concern would complicate any Western response. As this inchoate legal doctrine is further refined, several experts noted that individual companies are using "terms of use" and "terms of service" violations to remove particular bots, but this approach is not yet fast enough to address the pace at which new bots are created. In either event, debate continues about the potential costs of takedowns, in terms of resources and potential infringement of legitimate speech, in contrast to a greater emphasis on transparency and media literacy among the public.

...advances in computational power will likely make this challenge more significant in the immediate future.

Participants also noted how unauthorized access to sensitive information, such as voter registration or other voter data, could enhance micro-targeting at the local or even individual level, which often begins by promulgating information of local concern to build followers and trust before pivoting to areas of particular interest for Russia and its affiliates. While micro-targeting is used for legitimate purposes on social media sites, including by politicians seeking to target their constituents, nefarious uses of the practices include hacking legitimate accounts to spread disinformation, such as compromise of the Associated Press Twitter account in 2016, and stealing social media credentials to increase "likes" and views of particular social media pages.

Even as bot-driven disinformation or manipulation campaigns had perhaps inestimable impacts on the 2016 election, the Experts Group observed that advances in computational power will likely make this challenge more significant in the immediate future. Of note, improvements in artificial intelligence (AI) and human emulation will allow malicious actors to share (dis)information with increasing speed and scope while raising the difficulty of distinguishing bots from real people unless countervailing technologies are developed. Perhaps even more concerning, participants noted the development of technology capable of generating highly realistic audio and video files, further compounding the difficulty for the public to differentiate between real and fake sources. An additional complicating factor is that a substantial portion of information released during the 2016 presidential election was true, such as certain content from e-mails stolen from John Podesta, Hillary Clinton's campaign strategist, but the information was deployed selectively to affect the narrative, and potentially voting behavior, among specifically targeted groups.

The participants therefore identified four principal ways information operations can collectively undermine our fundamental democratic institutions: the willingness and capability of the adversary to share false information; the same willingness and capability to steal, corrupt, and deploy "true" information; the increasing capability of new technologies to disseminate, and even create, disinformation or misinformation at previously impossible speed and with precise micro-targeting; and the ongoing support of affinity groups, witting or unwitting, to amplify the adversary's chosen message.

04

Elements of a National Strategy

Ongoing investigations in the executive and legislative branches may shed more light on the active measures used by Russia in the 2016 election. In addition, governmental and nongovernmental discussions, and collaboration with other democracies similarly targeted by Russian active measures, will continue to further illuminate the methods and strategies for addressing them. However, the Experts Group concluded that enough is known already to provoke a sense of urgency in developing a national strategy to counter what is an ongoing threat, not just to upcoming elections, but to our fundamental institutions and support for liberal democracy. Such a strategy should be designed to prevent, deter, and reduce the effectiveness of future activities aimed at undermining our democratic processes and institutions.

...enough is known already to provoke a sense of urgency in developing a national strategy to counter what is an ongoing threat, not just to upcoming elections, but to our fundamental institutions and support for liberal democracy.

Prevent

There is little doubt that the Russian government, and potential copycat actors, will continue to leverage social and mass media platforms to affect the discourse of Western democracies. Such activities can be most effectively addressed, although not eliminated, by improved technical measures, including better cybersecurity and the ability to identify social media bots, as well as heightened transparency.

Social media platforms such as Facebook and Twitter have taken steps in removing both automated bots and disinformation from their platforms. These efforts must continue and may be appropriate for government investment, particularly in research and development. The arbiters of Internet platforms and the creators of disinformation are currently in an arms race to determine the future of online discourse. The United States and our allies must encourage social media platforms to make appropriate investments in reducing the prevalence and impact of automated bots and disinformation campaigns. Such encouragement may include financial support, research prioritization, and potentially consideration of an updated legal framework to mitigate concerns about legal liability. European countries are also considering robust measures to impose responsibility on social media companies.

Put simply, Internet platforms and democratic governments must work together on technological and policy measures to increase barriers to entry for disinformation campaigns and make it easier for citizens to differentiate between legitimate and false information. These technical measures must be accompanied by a campaign to help Americans understand why they should care and how they can become more discerning consumers of information,

particularly on the Internet. The U.S. government must also develop institutional processes and structures to share information about potential information operations with Internet platforms more quickly and with greater context.

Greater transparency in campaign finance, as well as business finance and economic transactions, can also reduce the ability of an adversary to corrupt our processes or sow doubt about their legitimacy, although these efforts face troubling political obstacles.

...the U.S. government must act urgently to secure our most sensitive infrastructures from direct interference.

Finally, the U.S. government must act urgently to secure our most sensitive infrastructures from direct interference. It has been publicly reported that Russian actors targeted electoral infrastructure in over 20 states prior to the 2016 election. Although there is no evidence indicating that these cyber operations resulted in the disruption of any voting results, the Russian government maintains both the intent and capability to undermine confidence in the integrity of an electoral tally. The need to increase cybersecurity among the nation's electoral infrastructure, and particularly in voter registration databases and electronic voting machines, has gained heightened salience since the 2016 election. Congress and the executive branch are challenged by the need to respect state authority over their electoral systems while recognizing the vulnerability created by systemic underinvestment in cybersecurity. Congress has the constitutional authority to determine the "time, place, and manner" of federal elections, and should consider leveraging this power to ensure strong cybersecurity measures and provide additional resources to help states institute necessary protections.

The *Defending Digital Democracy* Project, run out of Harvard University's Belfer Center, is working with election officials and campaigns to better secure their networks, share information on cyber threats, and implement best practices including security training and comprehensive response plans.

https://www.belfercenter.org/publication/cybersecurity-campaign-playbook.

In addition to improving network architecture, employees and officials must better understand the threat and steps they can take to reduce the likelihood that malicious cyber activity will result in a breach or disruption. Plans should be exercised and include scenarios in which an adversary could raise questions about the legitimacy of an election even without any successful cyber intrusion. An effective communications plan is an essential part of any comprehensive response plan.

Information operations already impact the U.S. judicial system, for example, using hot-button issues of refugees and concerns about racial justice.

Strengthening cybersecurity in other democratic institutions, including all three branches of government and the media, is also essential to mitigate the risk of foreign cyber attacks that may be designed to undermine public confidence.

Information operations already impact the U.S. judicial system, for example, using hot-button issues of refugees and concerns about racial justice.

Attacks on critical infrastructure also could be exploited for messaging purposes. For example, disruption of emergency communications during a crisis could have a significant impact on response and, as a result, may affect public confidence. Attacks on the electric grid, financial services, water, and many other sectors also could lead to questions about government competence, in addition to the direct impact from the attack.

Deter

Participants emphasized the need to increase the costs for entities that disrupt, or attempt to disrupt, fundamental democratic institutions. Bipartisan condemnation, from Congress and the administration, is necessary to send a clear message that continued interference is not acceptable. President Obama imposed limited sanctions and other punitive measures on Russia in December 2016. On August 2, 2017, President Trump took an important step in signing the congressionally enacted "Countering America's Adversaries Through Sanctions Act," which authorizes sanctions against any person or group who "knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation." The administration should use this authority to penalize entities determined to have targeted U.S. electoral infrastructure prior to the 2016 election and demonstrate that future activities targeting our democratic process and institutions will be met with crippling economic restrictions.

That said, imposing costs through the global financial system presents both asymmetric advantages and risk, and the group cautioned that U.S. policymakers must consider whether sanctions, at a certain point, lead to a higher likelihood of active measures against the U.S. financial system. An important area for further study is assessing how financial leverage can be more effectively used without turning the financial system into a battle space.

The group also suggested that other diplomatic, economic, and intelligence means should be considered to demonstrate clearly to Russia that continued efforts to undermine our democracy will not be tolerated. This could include both public and covert cyber actions, a "sunshine" information response that highlights problems in the Putin regime, or other technical measures, including interfering with Russian troll farms and bots. Like any deterrence measure, these carry a degree of risk that must be both considered and managed. U.S. practice should be guided by international law and evolving norms, including the UN's International Law Commission's draft law on countermeasures, to ensure that they can withstand public scrutiny.

...diplomatic, economic, and intelligence means should be considered to demonstrate clearly to Russia that continued efforts to undermine our democracy will not be tolerated.

Reduce Effectiveness of Active Measures

Increasing public resilience against the kinds of techniques used by Russia may ultimately be the most effective countermeasure. Disinformation campaigns and related tactics are most effective on a population inclined toward skepticism about their government officials and system. The Experts Group [therefore] suggested three approaches to enhancing societal resilience against information operations: increasing public understanding of the threat; promoting informed media consumption; and strengthening a sense of shared narrative around the value and importance of our democratic institutions.

The Experts Group [therefore] suggested three approaches to enhancing societal resilience against information operations: increasing public understanding of the threat; promoting informed media consumption; and strengthening a sense of shared narrative around the value and importance of our democratic institutions.

In the current political environment, the need to publicly acknowledge the extent of Russian interference in fundamental democratic institutions remains controversial. Nonetheless, the Experts Group agreed that widespread public understanding of the threat is a critical prerequisite to societal resilience. Government will play an important role in increasing public understanding, through the ongoing investigations and public statements, but figures outside of politics or government may be more trusted and compelling messengers. The American people must be aware that Russia, and potentially other foreign governments, seeks to undermine the strength and prosperity of the United States by degrading the integrity of our democratic processes and confidence in our democratic institutions, and that individuals are the most effective bulwark against such campaigns.

Attribution of cyber intrusions, such as those into the Democratic National Committee and John Podesta's e-mail, help illuminate the threat. Where government may be reluctant to name a perpetrator, to protect sources and methods for example, private researchers and cybersecurity firms have often stepped in to provide attribution. However, some firms are increasingly concerned about the risks to their business from naming nation-state actors. The group suggested that a consortium of companies that collectively provide attribution might mitigate this concern while providing important information for the public.

Of course, understanding the nature and extent of the threat is not enough. Media consumers should receive the tools and information to discriminate between "real" and "fake" information or sources, and between information posted by an actual person and by a bot. The government, Internet platforms, and media companies all have a role to play. Some states have begun to reinvigorate their media literacy, critical thinking, and civics curricula; more states should consider adopting such changes in K-12 schools. Universities and employers should consider adding courses and professional development programs to increase adults' skills in this area as well. Internet platforms are taking significant steps in "tagging" bots and removing identifiable fake news. Some Internet platforms are also implementing new systems where users can "rate" news sources based upon perceived trustworthiness, elevating the placement of trusted sources on the platforms' "news feeds." However, some experts argue these measures will further

ensconce users in filter bubbles and privilege legacy media platforms, demonstrating that the current media environment lacks a trusted arbiter of fact. Families no longer universally sit around the television each evening to receive delivered truth from network news anchors. Remaining local news outlets struggle to compete with larger outlets, creating a critical hole in coverage outside of major metropolitan areas. Individuals seek information from diffuse sources generally inflected by political or social preferences. The "mainstream" media outlets are no longer presumed to have a greater claim to accuracy than less established sources.

The challenge of media legitimacy and confirmation bias extends beyond concerns about Russian influence. However, greater transparency into the origins and intent of foreign sources may help media consumers make more conscious decisions. The decision to require RT, the Russian propaganda media outlet, to register as a foreign agent is one example of such an effort. Similarly, nonprofit organizations could begin to label media sources that are known to serve as a mouthpiece for, or to be controlled by, a foreign state. For example, the German Marshall Fund of the United States established "Hamilton 68," a tool to provide a near-real-time look at Russian propaganda and disinformation efforts online. Many Americans may no longer inherently trust the *New York Times* more than a recently founded website. But most Americans, one presumes, will place less credence in a Facebook post labeled as a front for the Russian government than an alternative source. Such an effort will inherently devolve into a cat-and-mouse game, with the advantage perhaps going to the producers of disinformation. But if the objective is less to eliminate disinformation and more to help voters weigh information more discreetly and with greater balance, the result will strengthen our democratic institutions.

Finally, participants emphasized that a sense of shared narrative is perhaps the strongest defense against Russian threats to our democratic institutions. If the American people can agree that we, as a nation, are bound by fundamental shared values despite our many differences; that we are made stronger because of the principles of democracy, inclusion, liberty, and individual rights; and that these principles are vital but fragile, we will find ways to withstand foreign attempts to weaken us. Conversely, if the American people perceive our national ideal to be mutable, or corrupted, or existing on a relative moral plane with Russia's illiberal autocracy, any technological or legislative intervention will fail. Reinvigorating our shared national narrative is therefore a generational imperative that requires democratic institutions live up to their responsibilities as pillars of democracy, and the engagement of educators, parents, elected officials, civil society, and, at a basic level, every American citizen.

Reinvigorating our shared national narrative is therefore a generational imperative that requires democratic institutions live up to their responsibilities as pillars of democracy, and the engagement of educators, parents, elected officials, civil society, and, at a basic level, every American citizen.

05

A Whole-of-Nation Campaign to Counter Foreign Adversary Threats to Democratic Institutions

America's fundamental democratic institutions are at risk. The Russian government is engaged in a covert and overt campaign to weaken Western democracies, with the express intent of promoting an illiberal order dominated by Moscow and like-minded states. And yet, the executive branch is not fully engaged in this challenge. Activities that may exist across the U.S. government are inchoate, inconsistent, and disorganized. Countering foreign adversary information operations inside the United States challenges our current organizational framework. The intelligence community is limited in what it can do inside the United States, particularly regarding influence operations. The FBI is focused on the counterintelligence aspects but not leading a proactive public campaign, nor would we expect it to. The Department of Homeland Security (DHS) may be a logical choice but has not been given the mission.

The United States requires a National Strategy to Counter Foreign Adversary Threats to Democratic Institutions.

The United States requires a *National Strategy to Counter Foreign Adversary Threats to Democratic Institutions*. If the administration is not ready to lead development of such a strategy, it must be created and implemented by concerned individuals in Congress, the judiciary, state and local governments, civil society, and the private sector. This strategy, in brief, must outline how to respond to the "Kremlin playbook" as implemented in the United States and as it may be adapted by other adversaries. This campaign should include five goals:

1. Publicize the extent of Russian, and potentially other adversaries', interference in democratic institutions and increase awareness of the threat within those institutions and among the public.

2. Promote bipartisan action against Russia and its proxies, and increase technical defenses and countermeasures, to increase the costs of disruptive activities.

3. Improve transparency into foreign adversary interference through measures such as campaign finance reform, foreign agent disclosure, and tagging adversary-operated "bots."

4. Research the extent to which specific adversary techniques, including cyber-enabled activities, influence public opinion and target mitigation approaches to address the most damaging techniques.

5. Engage in a national effort to promote and reinvigorate American understanding of the importance of democracy and our democratic institutions, as a bulwark against foreign efforts to exploit divisions and complacency. This should include media literacy, critical thinking, and civics curricula at all levels, updated for the digital age.

The threats outlined in this report are the latest front in an enduring struggle between liberalism and illiberalism, between autocracy and democracy, between liberty and oppression. It is not clear that liberalism and democracy are winning: recent research reveals that younger citizens in long-standing democracies are "less likely to consider it essential to live in a democracy than earlier cohorts." But the significance of this threat has not yet penetrated the psyche of the American people. This report is therefore a call to action. The experts who contributed to this report have already begun, in a variety of ways, to work with government, private-sector, and civil society partners to advance efforts that can inform and help implement a *National Strategy to Counter Foreign Adversary Threats to Democratic Institutions*. All Americans, regardless of political affiliation or ideological grounding, should feel compelled to join in this critical effort.

Annex A: Agenda and List of Participants for Expert Roundtables

June 20, 2017

Rapporteur: Eric Goldstein

Agenda:

- Welcome/Introductions – Dr. John Hamre and Suzanne E. Spaulding
- Topic 1: Nature and Scope of the Threat – Led by Heather Conley
- Topic 2: Vulnerabilities That Russia Can and Does Exploit – Led by Michael Chertoff
- Topic 3: Discussion about Possible Actions to Counter
- Topic 4: Next Steps

List of Participants:

- John Hamre, *President and CEO, CSIS*
- Suzanne E. Spaulding, *former Under Secretary, DHS*
- John Bellinger, *former NSC and State Legal Adviser*
- Michael Chertoff, *former Secretary, DHS*
- Matt Chessen, *Foreign Service Science, Technology and Foreign Policy Fellow, Center for International Science and Technology Policy, GWU*
- Frank Cilluffo, *Director, Center for Cyber and Homeland Security, GWU*
- David S. Cohen, *former Deputy Director, CIA, and former Assistant Secretary, Treasury*
- Heather Conley, *Senior Vice President for Europe, Eurasia, and the Arctic and Director of the Europe Program at CSIS*
- Mary DeRosa, *former NSC Legal Adviser*
- Michele Flournoy, *former Under Secretary of Defense for Policy*
- Siobhan Gorman, *former Wall Street Journal reporter*

- Jim Lewis, *director of CSIS's Technology and Public Policy Program*
- John MacGaffin, *former Associate Deputy Director for Operations/CIA, Senior Adviser to FBI Director, and Chair of CI-21*
- Holly McMahon, *ABA Standing Committee on Law and National Security*
- Jeffrey Rathke, *Deputy Director, Europe Program, CSIS*
- Eric Rosenbach, *Codirector, Belfer Center for Science and International Affairs, Harvard Kennedy School*
- Laura Rosenberger, *Senior Fellow, German Marshall Fund, and former Chief of Staff to Deputy Secretary of State*
- David Sanger, *New York Times reporter*
- Neal Wolin, *former Deputy Secretary of Treasury*

December 13, 2017

Rapporteur: Joseph P. Federici

Agenda:

- Welcome/Introductions – Suzanne E. Spaulding
- Brief Presentations:
    - Eric Rosenbach, Codirector, Belfer Center for Science and International Affairs, on the *Defending Digital Democracy Initiative*
    - Laura Rosenberger, The German Marshall Fund, on the *Alliance for Securing Democracy*
    - Michael Hayden, Former Director, CIA and Director, NSA, on the *Committee to Investigate Russia* and "The Future of Truth" panel at the Nobel Week Dialogue in December 2017, https://www.youtube.com/watch?v=-ckLJnclPiw
    - Suzanne E. Spaulding, Former Under Secretary, National Protection and Programs Directorate, DHS, and CSIS, on *Countering Adversary Attacks on America's Justice System*
    - Meryl Chertoff, Executive Director of The Aspen Institute's Justice and Society Program on efforts to defend the judiciary
- Discussion

List of Participants:

- John Bellinger, *former NSC and State Legal Adviser*
- Meryl Chertoff, *Aspen Institute*
- Heather Conley, *CSIS*
- Geysha Gonzalez, *Atlantic Council*
- Ken Gude, *Center for American Progress*
- Michael Hayden, *Former NSA Director and CIA Director*
- David Heyman, *Aspen Institute*
- Nina Jankowicz, *Wilson Center, Kennan Institute*
- James Lewis, *CSIS*
- John MacGaffin, *Former CIA*
- Holly McMahon, *ABA Standing Committee on Law and National Security*
- Jeff Rathke, *CSIS*
- Harvey Rishikof, *ABA Standing Committee on Law and National Security*
- Eric Rosenbach, *Codirector, Belfer Center for Science and International Affairs, Harvard Kennedy School*
- Laura Rosenberger, *Senior Fellow, German Marshall Fund, and former Chief of Staff to Deputy Secretary of State*
- Paul Rosenzweig, *R Street Institute*
- David Sanger, *New York Times reporter*
- Loren Shulman, *Center for a New American Security*
- Suzanne E. Spaulding, *CSIS, former Under Secretary, DHS*

Annex B: Links to Expert Group Projects

- Meryl Chertoff, Aspen Institute Justice and Society Program. The program convenes individuals from diverse backgrounds to discuss the meaning of justice and how a just society ought to balance fundamental rights with the exigencies of public policy, in order to meet contemporary social challenges and strengthen the rule of law. See, for example, *Pluralism in Peril: Challenges to an American Ideal.* https://www.aspeninstitute.org/events/inclusive-america-project-report-launch-pluralism-peril-challenges-american-ideal/; https://www.aspeninstitute.org/programs/justice-and-society-program/.

- Michèle Flournoy, former president/current board member, and Loren Schulman, deputy director of studies, Center for a New American Security. The Center for a New American Security (CNAS) is leading two parallel efforts related to disinformation threats. First, CNAS is hosting a series of off-the-record roundtables in the policy and academic communities exploring the national security implications of digital disinformation, allowing experts to highlight their specific work. Second, CNAS is leading an effort exploring how the national security policy and technology communities collaborate on hard problems, using lessons from a year of research to take on digital disinformation. https://www.cnas.org/.

- Geysha Gonzalez, associate director, Dinu Patriciu Eurasia Center, The Atlantic Council. The Atlantic Council's Eurasia Center's work on disinformation is designed to galvanize the public, nongovernmental, and private sectors of the transatlantic community to respond to the global challenge of disinformation posed by radical groups and hostile regimes. To advance these efforts, the Council not only produces cutting-edge research and publish timely analysis, but it also seeks to build a strong, transatlantic network that encompasses key policymakers, civil society, journalists, and private-sector leaders. http://www.atlanticcouncil.org/.

- Michael Hayden, Advisory Board, Committee to Investigate Russia. The Committee to Investigate Russia is a nonprofit, nonpartisan resource provided to help Americans recognize and understand the gravity of Russia's continuing attacks on our democracy. All relevant information is aggregated in one place to provide context and allow users to see the full picture of what Russia has done and will continue to do unless we start paying closer attention. https://investigaterussia.org/.

- Nina Jankowicz, former George F. Kenna Fellow at the Wilson Center and strategic communications adviser to the Ukrainian Foreign Ministry. Researching the evolution of modern Russian information warfare in Central and Eastern Europe over the last 10 years. https://www.wilsoncenter.org/person/nina-jankowicz

- James Lewis, senior vice president, Center for Strategic and International Studies. This project examines how cyber operations produce cognitive effect to manipulate public opinion and political leaders and how cybersecurity strategies should be adjusted to deter or respond to this. https://www.csis.org/analysis/rethinking-cybersecurity.

- Eric Rosenbach, codirector, Belfer Center for Science and International Affairs, Defending Digital Democracy. The Defending Digital Democracy project aims to develop strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks. https://www.belfercenter.org/D3P.

- Laura Rosenberger, The German Marshall Fund, Alliance for Securing Democracy. The Alliance for Securing Democracy, a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States, will develop 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 will work to publicly document and expose Vladimir Putin's ongoing efforts to subvert democracy in the United States and Europe. http://securingdemocracy.gmfus.org/.

- Paul Rosenzweig, senior fellow, R Street Institute, Election Security Initiative. The initiative focuses on enhancing the structural cybersecurity of the electoral system through cooperative federal-state efforts involving information sharing, resource allocation, and standard setting. www.rstreet.org/electioncyber.

- Suzanne E. Spaulding, senior adviser, Center for Strategic and International Studies, Countering Adversary Attacks on America's Justice System. The project is focused on assessing and countering Russian activities that can undermine public faith and confidence in the justice system as an essential pillar of democracy. https://www.csis.org/.

About the Authors

Suzanne E. Spaulding is a senior adviser to the Homeland Security Program and International Security Program at the Center for Strategic and International Studies, where she leads the project on Countering Threats to the Fundamental Institutions of Democracy. She is a former undersecretary in the U.S. Department of Homeland Security.

Eric Goldstein is a 2017 cyber fellow at the Center for Strategic and International Studies. He is also an attorney in the data security and privacy practice at O'Melveny & Myers LLP. Previously, he served as branch chief for partnerships and engagement in the U.S. Department of Homeland Security's Office of Cybersecurity and Communications.

COVER PHOTO ANDREAS SOLARO/AFP/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org